**ÖGER Research Paper Series**

**Nr. 1/2020**

# „Industrie 4.0 im Maschinen- und Anlagenbau – rechtliche Herausforderungen in der EU im Überblick“

verfasst von
Matthias Grosinger

Wien, 2020

https://deicl.univie.ac.at/team/jaeger-thomas/oesterr-gesellschaft-f-europarecht/

**Inhaltsverzeichnis**

**Abkürzungsverzeichnis**

| | |
|---|---|
| AGB | Allgemeine Geschäftsbedingungen |
| ABGB | Allgemeines Bürgerliches Gesetzbuch, JGS 1811/946 |
| Abs | Absatz |
| AEUV | Vertrag über die Arbeitsweise der Europäischen Union |
| Art | Artikel |
| BGB | Bürgerliches Gesetzbuch |
| BGBl | Bundesgesetzblatt |
| BMWi | Bundesministerium für Wirtschaft und Energie |
| bzgl | bezüglich |
| bzw | beziehungsweise |
| B2B | Business-to-Business |
| B2C | Business-to-Consumer |
| CEN | Comité Européen de Normalisation (Europäisches Komitee für Normung) |
| $CO_2$ | Kohlendioxid |
| Dako | Datenschutz konkret |
| dh | das heißt |
| DSGVO | Datenschutzgrundverordnung |
| DJZ | Deutsche Juristenzeitung |
| ecolex | Fachzeitschrift für Wirtschaftsrecht |
| EDPB | European Data Protection Board |
| EG | Europäische Gemeinschaft |
| ENISA | European Union Agency for Cybersecurity |
| etc | et cetera („und die übrigen [Dinge]“) |
| EU | Europäische Union |
| EuGH | Europäischer Gerichtshof |
| EUV | Vertrag über die Europäische Union |
| EWG | Europäische Wirtschaftsgemeinschaft |
| f | folgende |
| ff | fortfolgende |
| FKVO | Fusionskontrollverordnung |
| F&E | Forschung und Entwicklung |
| ggfls | gegebenenfalls |

| | |
|---|---|
| GVO | Gruppenfreistellungsverordnung |
| Hrsg | Herausgeber |
| IaaS | Infrastructure as a Service |
| IEC | Internationale elektrotechnische Kommission |
| IoT | Internet of Things (Internet der Dinge) |
| IIoT | Industrial Internet of Things |
| iSd | im Sinne des, - der |
| ISO | Internationale Organisation für Normung |
| IT | Informationstechnik |
| jusIT | Zeitschrift für IT-Recht, Rechtsinformation und Datenschutz |
| KI | Künstliche Intelligenz |
| KMU | Klein- und Mittelunternehmen |
| lit | litera (Buchstabe) |
| M&A | Mergers & Acquisitions |
| NJW | Neue Juristische Wochenschrift |
| Nr | Nummer |
| oÄ | oder ähnliche(s) |
| ÖJZ | Österreichische Juristenzeitung |
| PaaS | Platform as a Service |
| PKW | Personenkraftwagen |
| RL | Richtlinie |
| Rs | Rechtssache |
| Rn | Randnummer |
| Rz | Randzahl |
| SaaS | Software as a Service |
| SLA | Service Level Agreement |
| ua | unter anderem |
| UG | Universitätsgesetz 2002, BGBl 120/2002 |
| VO | Verordnung |
| vzbv | Verbraucherzentrale Bundesverband e.V. |
| Z | Ziffer |
| Zak | Zivilrecht Aktuell |
| zB | zum Beispiel |

# 1 Einleitung

In vielen Bereichen unserer Gesellschaft findet eine fortschreitende Entwicklung von IoT (Internet of Things)[1]-Lösungen, eine weitreichende Vernetzung und damit einhergehend ein intensiver Austausch von Daten statt. Sowohl im Alltag vieler Verbraucher, als auch bei komplexen Industrieanlagen haben Daten und Systeme, welche enorme Datenmengen speichern, auswerten und/oder verarbeiten, eine zentrale und nicht mehr wegzudenkende Rolle eingenommen. Angesichts der unternehmerischen Chancen und dem erwarteten Mehrwert ist der Besitz dieser gesammelten Daten für viele Unternehmen verlockend, in rechtlicher Hinsicht aber auch sehr komplex.

## *1.1 Forschungsfrage*

Der Hintergrund dieser Master Thesis ist ein Industrie 4.0 Projekt, welches durch das Unternehmen, in welchem ich tätig bin, aktuell bearbeitet, entwickelt und an ersten Anlagen bereits getestet wird. Das Unternehmen liefert industrielle Wärmebehandlungsanlagen für sämtliche Branchen und möchte seine Marktposition durch die Erweiterung des Produkt-Portfolios auf Industrie 4.0-Technologien, wobei der Fokus auf unterstützenden Instandhaltungs- und Wartungsanwendungen liegt, stärken. Neben den neuen technischen und technologischen Herausforderungen dieser Entwicklung ist das Ziel dieser Master Thesis, die rechtlichen Herausforderungen wissenschaftlich zu untersuchen, einen Überblick über die derzeitige Rechtslage sowie mögliche Handlungsempfehlungen zu geben.

Im Rahmen dieser Master Thesis wird diese komplexe rechtliche Komponente im europäischen Kontext näher betrachtet, um Antworten auf die Forschungsfrage geben zu können, welche Rechte Hersteller und Kunden von digitalen Anwendungen im Maschinen- und Anlagenbau haben und welche erforderlichen vertraglichen Regelungen vorzusehen sind um umfassenden Rechtschutz zu erhalten.

[1] *Raffling/Schock (Hrsg)*, Digitale Wirtschaft und Industrie 4.0 (2018) 220f.

## *1.2 Erwartete Ergebnisse/Ziele der Arbeit*

Diese Master Thesis soll im Zusammenhang mit IoT und im Speziellen IIoT (Industrial Internet of Things)[2] einen Überblick über die bereits vorhandenen Regulierungen und die damit verbundenen neuen rechtlichen Herausforderungen geben. Die vorliegende Arbeit beschränkt sich in der Diskussion auf die mit industriellen IoT-Lösungen in Verbindung stehenden auswählten Rechtsgebiete. Auf die weiteren betroffenen Rechtsgebiete kann im Rahmen dieser Arbeit nicht bzw. nur am Rande eingegangen werden.

### 1.2.1 Übersicht der rechtlichen Herausforderungen

Die komplexen rechtlichen Herausforderungen, welche die Digitalisierung mit sich bringt, sind sehr vielfältig und umfassen verschiedenste Rechtsgebiete. Beispielsweise spielen das AGB-Recht, das Vertragsrecht und neue Vertragsmodelle, das Datenschutzrecht, das Urheberrecht, das Arbeitsrecht, das IT-Sicherheitsrecht, das Kartell- und Wettbewerbsrecht und das Haftungsrecht neben anderen Rechtsgebieten eine Rolle bei IoT-Anwendungen im Maschinen- und Anlagenbau.

Die rasante Entwicklung der Digitalisierung und die steigende Nachfrage an automatisierten Systemen in der Industrie machen es der modernen Jurisdiktion, sowohl national als auch international, schwer Schritt zu halten und geeignete rechtliche Rahmenbedingungen bereitzustellen.

In den letzten Jahren gibt es sowohl in der europäischen Union selbst, als auch in vielen Mitgliedstaaten der europäischen Union Bestrebungen einen angepassten Rechtsrahmen für die digitale Welt zu schaffen. Die geänderten Voraussetzungen des digitalen Raumes erfordern die Umsetzung entsprechender richtungsweisender Maßnahmen, um mit einer soliden Rechtsbasis eine sichere und geregelte Entwicklung des digitalen Binnenmarktes zu gewährleisten. Die Europäische Kommission hat bereits Richtlinienvorschläge für ein mögliches harmonisiertes neues Vertragsrecht im digitalen Binnenmarkt erarbeitet und eine digitale Strategie für Europa vorgestellt.[3] Auf nationaler Ebene haben beispielsweise

[2] *Raffling/Schock (Hrsg)*, Digitale Wirtschaft und Industrie 4.0 (2018) 221.
[3] *Europäische Kommission*, COM(2015) 192 final 1ff.

Deutschland die „Digitale Agenda 2014 – 2017“[4] bzw. Österreich die Webplattform „Digital Austria“[5] ins Leben gerufen, um den neuen digitalen Anforderungen gerecht zu werden. Erste Maßnahmen aus diesen Strategiepapieren, wie beispielsweise die Anpassung des Rechtsrahmens (in Deutschland) im Zuge der Strategie automatisiertes und vernetztes Fahren[6], wurden bereits umgesetzt.

Solange es jedoch keine umfassende einheitliche europäische Rechtsgrundlage gibt bzw. keine Gesetzgebungsvorschläge umgesetzt sind, welche alle neuen Herausforderungen der digitalen Welt abdecken, bleibt es die Aufgabe der einzelnen Vertragsparteien bzw. der Unternehmen die vorhandenen Unsicherheiten im Sinne der Privatautonomie vertraglich zu regeln, um so Risiken für das Unternehmen im Hinblick auf die rechtlichen Grauzonen der Digitalisierung zu minimieren.

Diese Master Thesis soll einen Beitrag zur aktuellen rechtswissenschaftlichen Diskussion leisten und einen Überblick über die verfügbare Literatur geben. Anhand der Methode der Rechtsinterpretation (Rechtsanwendung) sollen mögliche Regulierungsansätze für die Auseinandersetzung mit diesen neuen digitalen rechtswissenschaftlichen Themen in Zusammenhang mit Industrie 4.0-Lösungen erarbeitet werden.

### 1.2.2 Vertragliche Regelungen im B2B-Bereich

Die umfassenden Fragestellungen, welche die Digitalisierung mit sich bringt, zwingt Unternehmen in B2B (Business-to-Business) Geschäftsbeziehungen spezifische vertragliche Regelungen vorzusehen.

Im Falle von IIoT-Anwendungen sind Daten, neben dem geistigen Eigentum des Kunden (in diesem Zusammenhang ist der Kunde ein anderer Unternehmer), das wichtigste zu schützende Gut. Sensoren, Aktoren und weitere intelligente Bauteile liefern Informationen in Form von Daten von produzierenden Maschinen und Anlagen, welche üblicherweise die Grundlage für

[4] *Bundesministerium des Innern / Bundesministerium für Wirtschaft und Energie / Bundesministerium für Verkehr und digitale Infrastruktur*, Legislaturbericht Digitale Agenda 2014-2017 (2017) 4ff.
[5] *Österreichische Forschungsförderungsgesellschaft mbH*, Die digitale Strategie der österreichischen Bundesregierung, https://www.digitalaustria.gv.at/
[6] *Bundesministerium des Innern / Bundesministerium für Wirtschaft und Energie / Bundesministerium für Verkehr und digitale Infrastruktur*, Legislaturbericht Digitale Agenda 2014-2017 (2017) 56.

ein IT-gestütztes System zur Analyse und Dokumentation von Maschinenzuständen sowie zur Optimierung von Produktionsprozessen darstellen.

Beurteilt man die Bedeutung der einzelnen rechtlichen Themenfelder für Hersteller von IIoT-Lösungen sowie für ihre Kunden, so kann man annehmen, dass der Datenschutz, die Datensicherheit sowie das Dateneigentum im Vordergrund einer vertraglichen Regelung zwischen Unternehmen stehen.
Der Vertrag muss sich u.a. mit den folgenden Fragen auseinandersetzen und Bedingungen zur Regelung dieser beinhalten:

- Wer ist der rechtmäßige Eigentümer der Daten?
- Wer hat das Recht die Daten zu nutzen (speichern, verarbeiten, löschen, etc.)?
- Wo werden die Daten gespeichert?
- Werden automatisierte Vertragsabschlüsse durchgeführt (z.B. ein defekter Sensor wird erkannt und automatisch nachbestellt)?
- Wie sicher sind die Daten (IT-Datenschutz)?
- Wer haftet bei Fehlern und daraus resultierenden Schäden?

Bevor diese Fragen beantwortet bzw. vertragliche Regelungen für diese Fragestellungen formuliert werden können, muss eingehend geklärt werden, um welche Art von Daten es sich im konkreten Sachverhalt handelt. Neben der Verarbeitung von personenbezogenen Daten, welche durch die Datenschutz-Grundverordnung (DSGVO) geregelt wird, sind bei IIoT-Systemen vor allem nicht-personenbezogene Daten wie zum Beispiel Maschinen- oder Prozessdaten von Bedeutung. Die Verarbeitung dieser nicht-personenbezogenen Daten werden von der DSGVO nicht betrachtet.

# 2 Industrie 4.0 / Digitale Lösungen im Maschinen- und Anlagenbau

Diese Master Thesis beschäftigt sich im Speziellen mit dem Anwendungsfeld von IIoT-Lösungen in Form von Instandhaltungs- und Wartungsanwendungen im Maschinen- und Anlagenbau. Um die Forschungsfrage zu beantworten, widmet sich deshalb das dritte Kapitel der terminologischen Klärung und einem Ausblick auf die rechtlichen Rahmenbedingungen.

## *2.1 Definition und Zusammenhang*

Angesichts der Tatsache, dass die Produktion mit mechanisch bzw. händisch angetriebenen Arbeitsmaschinen häufig eine sehr schwere körperliche und dadurch auch ineffiziente und fordernde Arbeit ist, fand vor dem Hintergrund sich die Arbeit in der Produktion zu erleichtern die erste industrielle Revolution (Industrie 1.0) mit der Entwicklung der Dampfmaschine Ende des 18. Jahrhunderts statt. In vielen Industriebereichen, sowie in der Landwirtschaft und als Transportmittel setzte sich die Dampfmaschine als Antrieb immer mehr durch. Ende des 19. Jahrhunderts wurde die Dampfmaschine teilweise durch den Elektromotor abgelöst und die sogenannte zweite industrielle Revolution (Industrie 2.0) ermöglichte die industrielle Massenproduktion mit Hilfe von Elektrizität. Die nächste Entwicklungsstufe, die dritte industrielle Revolution oder digitale Revolution (Industrie 3.0), fand in den 1970er Jahren mit Automatisierung von Produktionsanlagen durch Computertechnologien (IT und Elektronik) statt. Neben der Industrie wurde auch der Dienstleistungsbereich von der neuen Technologie revolutioniert und Prozesse in allen Bereichen weitreichend optimiert. Die Errungenschaften der drei vorangegangenen industriellen Revolutionen sind bis heute omnipräsent und bilden das Fundament für die sogenannte vierte industrielle Revolution (Industrie 4.0). Das produzierende Gewerbe, im Speziellen der Maschinen- und Anlagenbau sowie die Automobilindustrie, sind die treibenden Kräfte in der Entwicklung und Anwendung der neuen digitalen Technologien.[7]

Diese aktuelle Entwicklungsstufe versucht durch neue Technologien und vor allem durch die Digitalisierung die Produktionsprozesse zu optimieren, indem Informationen aus sämtlichen Schnittstellen zwischen Mensch, Maschine sowie der gesamten Wertschöpfungskette erfasst,

[7] *Raffling/Schock (Hrsg)*, Digitale Wirtschaft und Industrie 4.0 (2018) 2.

analysiert und verarbeitet werden. Die Vernetzung all dieser Komponenten, Maschinen, Menschen etc. wird mit dem Begriff „Internet der Dinge (IoT)“ definiert. In diesem Zusammenhang sind „Dinge“, die „Gegenstände“, d.h. im industriellen Umfeld zum Beispiel Sensoren, Aktoren, intelligente Endgeräte etc., welche Daten von Maschinen erfassen und diese via Internet oder über andere moderne Medien kommunizieren. Diese Vernetzung wird genutzt um spezifische Informationen über Einzelkomponenten, Maschinen, Prozesse und deren reale Zustände zu erhalten, welche dann gespeichert, analysiert und weiterverarbeitet werden können. Die Verarbeitung dieser enormen Datenmengen, welche vielfach mittels komplexer Software-Unterstützung durchgeführt wird, bezeichnet man häufig als „Big Data“[8]. Angesichts der Möglichkeit, dass in diesen Prozessen mehrere unterschiedliche Parteien involviert sein können und die Daten womöglich von verschiedenen Personen an unterschiedlichen Orten verarbeitet werden können, sind die rechtlichen Themen Datenschutz, Datensicherheit und Dateneigentum von grundlegender Bedeutung im Bereich Industrie 4.0.

Industrie 4.0, IIoT bzw. digitale Lösungen im Maschinen- und Anlagenbau befinden sich derzeit noch in einer Entwicklungsphase, weshalb in diesem Zusammenhang auch die rechtliche Komponente noch sehr undurchsichtig ist und viele Fragen offenbleiben. Dies ist dem Umstand geschuldet, dass sowohl nationale als auch europaweite Rechtsgrundlagen im spezifischen Umfeld von Industrie 4.0-Anwendungen erst im Entstehen sind und bis dato nur vereinzelt bzw. für ganz spezifische Fälle, Sachverhalte in Zusammenhang mit der Digitalisierung ausjudiziert wurden.

## *2.2 Industrial IoT-Instandhaltungs- und Wartungsanwendungen*

Die weltweit wachsenden Märkte und Industrien sowie der zunehmende Wettbewerbsdruck stellen die europäische Industrie vor große Herausforderungen. Flexibilität der Unternehmen, Unterstützung durch die Politik und eine modernes Rechtssystem sind notwendig, um die internationale Wettbewerbsfähigkeit und Europas Wirtschaft wieder zu stärken.

Eine Möglichkeit um den Produktionsstandort weltweit weiter zu behaupten bietet sich durch den Einsatz von Industrie 4.0 Lösungen. Die Steigerung der Verfügbarkeit der Maschinen und

[8] *Raffling/Schock (Hrsg)*, Digitale Wirtschaft und Industrie 4.0 (2018) 219f.

Anlagen, die raschere Weiterentwicklung und Steigerung der Qualität der Produkte sollen durch den Einsatz neuer Technologien ermöglicht werden.
Der Einsatz unterstützender digitaler Systeme in der produzierenden Industrie soll die Steigerung der Flexibilität, Qualität, Prozesssicherheit, Produktivität und der Wettbewerbsfähigkeit gewährleisten. Der Überbegriff für eine solche digitale, vernetzte und flexible Produktion ist die sogenannte „Smart Factory“[9].

Eine der Instandhaltungs- und Wartungsanwendungen, welche in dieser Master Thesis betrachtet wird, ist „Predictive Maintenance“[10]. Diese Technologie nutzt den vorausschauenden Ansatz für die Wartung und Instandhaltung von Maschinen und Anlagen.

Die Kernaufgaben dieses Tools gliedern sich in das Auswerten und Analysieren von Daten, um folgend auf Basis der Resultate von Trendanalysen, statistischen Methoden und Erfahrungswerten, Vorhersagen über mögliche zukünftige Ereignisse treffen zu können. Eine erwartete höhere Wettbewerbsfähigkeit und niedrigere Kosten durch effizientere Systeme, Prozesse und verbesserte Qualität durch rechtzeitiges Erkennen von möglichen Störfaktoren im Prozess und die Verringerung von ungeplanten Anlagenstillständen durch ein individuell angepasstes Grenzwert-Management, sind weitere gängige Elemente einer Predictive Maintenance Anwendung. Im gesamtheitlichen Kontext dient das Tool auch der Förderung des länder- und standortübergreifenden Daten- und Erfahrungsaustausches innerhalb des digitalen Binnenmarktes.[11]

Das Fundament für eine Predictive Maintenance-Anwendung sind die Daten und Anlagenzustände, welche von Sensoren oder Aktoren erfasst, kommuniziert und dann mittels Condition Monitoring in Echtzeit aufgezeichnet werden. Aufgrund von Erfahrungswerten werden Grenzwerte vorgegeben und ergänzend durch Analyse von Trends, der „Gesundheitszustand“ der Anlagenkomponente bzw. Maschine festgestellt.

[9] Unter Smart Factory versteht man die vernetzte industrielle Produktion oder intelligente Fabrik, in welcher Produktionsprozesse, durch den Einsatz von IoT und den regen Austausch von Daten, automatisiert und ohne den Eingriff von Menschen ablaufen.
[10] *Synek/Feldmann/Herweg/Rauen*, Predictive Maintenance, Service der Zukunft – und wo er wirklich steht (2017) 3.
[11] Praxisbeispiel: Im Bereich von Wärmebehandlungsanlagen wird Predictive Maintenance dazu eingesetzt, um auf Basis von Sensordaten präzise Ausfallsvorhersagen zu treffen und dadurch kostenintensive Anlagenstillstände zu vermeiden.

Eine Form den Gesundheitszustand von Anlagenkomponenten zu bewerten und visualisieren ist mittels der unterschiedlichen Signale eines mehrphasigen Ampelsystems. D.h. auf Basis von vorgegebenen Grenzwerten ändert sich die Farbe der Ampel auf Rot, Orange oder Grün. Die Farben der Ampel geben nur eine Indikation für den Zustand der Komponente (z.B. Grün = OK ; Orange = Warnung, das Teil ist zu überprüfen bzw. eine Wartung durchzuführen ; Rot = Achtung, das Teil zeigt ein Verhalten abweichend zu den Erfahrungswerten – Teil überprüfen, warten und ggfls. austauschen), jedoch keine verbindliche Anweisung an Nutzer der Industrie 4.0-Anwendung weiter.

Eine weitere Funktion von IIoT Instandhaltungs- und Wartungsanwendungen ist die Erinnerungsfunktion zur Durchführung von vorgeschriebenen Wartungen entsprechend der vordefinierten Wartungsintervalle des Herstellers. Es funktioniert so, dass Wartungshinweise auf Basis einer Dokumentation von Einzelkomponenten oder Anlagen (Basis: Betriebs- oder Wartungsanleitung) in Abhängigkeit von der Nutzungsdauer und der Zeitspanne zur zuletzt durchgeführten Wartung an den Nutzer der Industrie 4.0-Anwendung weitergegeben werden. Um diese Auswertungen durchzuführen sind nicht unbedingt maschinengenerierte Daten erforderlich, da diese Betriebszeiten zumeist auch über ein Prozessleitsystem abgerufen werden können und mit den elektronisch gespeicherten Wartungsinformationen aus der Dokumentation verglichen werden. Spezifische maschinengenerierte Daten sind dann erforderlich, wenn für Komponenten Vorhersagen zur Lebensdauer oder Ausfallswahrscheinlichkeit gemacht werden sollen.

Im Rahmen des Entwicklungsprojekts in meinem Unternehmen ist eine weitere innovative Zusatzfunktion der Industrie 4.0-Anwendung die Identifizierung von Anlagenkomponenten (Sensoren, Aktoren, etc.) mittels Bilderkennung. Ein mit einem Tablet durch den Nutzer erzeugtes Bild wird an einen Server gesendet (nicht gespeichert) und mit den verfügbaren Komponenten abgeglichen. Bei einem positiven Abgleich werden über eine App am Tablet die verfügbaren ausgewerteten Daten (z.B.: Gesundheitszustand oder Trends) zu dieser Komponente mittels der Condition Monitoring Funktion angezeigt. Zusätzlich besteht die Möglichkeit auf die elektronische Dokumentation zuzugreifen oder die Wartungsintervalle einzusehen.

Diese neuen digitalen Anwendungen bieten eine große rechtliche Angriffsfläche, speziell wenn es um die Handhabung von Daten oder um die Schutzrechte der Nutzer und Hersteller geht.

Welche juristischen Konsequenzen die Implementierung einer Industrie 4.0-Anwendung hat und wie Verträge rechtskonform gestaltet werden können, ist Gegenstand der nachfolgenden Untersuchung im Rahmen dieser Master Thesis.

## *2.3 Rechtliche Rahmenbedingungen*

Die Beschreibung der IIoT-Anwendungen im letzten Abschnitt 3.2 und deren Kernfunktionen lassen die vielseitigen und komplexen rechtlichen Herausforderungen erahnen. Die Master Thesis beschränkt sich bei der Betrachtung der rechtlichen Rahmenbedingungen ausschließlich auf die europäischen primärrechtlich (EUV, AEUV) und sekundärrechtlich (EU-Verordnungen, EU-Richtlinien) maßgeblichen Rechtsvorschriften.

Es werden vorrangig die EU-Rechtsvorschriften für den digitalen Binnenmarkt, welche IIoT-Anwendungen betreffende Regulierungen beinhalten, behandelt und gemäß dieser Rechtsgrundlagen Gestaltungsspielräume für die Vertragsgestaltung evaluiert. Vorwiegend stützt sich die Untersuchung auf rechtliche Rahmenbedingungen, welche den Hersteller von IIoT-Anwendungen tangieren könnten.

Dazu zählen allen voran das Kartell- und Wettbewerbsrecht, mit Bestimmungen, die den Marktzutritt für Unternehmen regulieren, das Datenschutzrecht, das Urheberrecht und das Haftungsrecht.

# 3 Industrie 4.0 Lösungen im digitalen Binnenmarkt

Das folgende Kapitel setzt sich mit dem Einsatz von Industrie 4.0 Lösungen im digitalen Binnenmarkt auseinander. Zunächst wird versucht einen Überblick über die wichtigsten EU-Rechtsvorschriften in diesem Zusammenhang zu geben und diese zu interpretieren. Anschließend setzt sich dieses Kapitel mit der Analyse des Kartell- und Wettbewerbsrechts und den Auswirkungen auf Industrie 4.0 Lösungen auseinander.

## *3.1 Übersicht der EU-Gesetzgebung im digitalen Binnenmarkt*

Der Grundgedanke in der Wirtschaftsstrategie der europäischen Union ist es einen gemeinsamen Markt zwischen den Mitgliedstaaten zu realisieren. Die tatsächliche und vollumfängliche Verwirklichung des sogenannten gemeinsamen Binnenmarktes stellt die Europäische Union und ihre Mitgliedstaaten vor große Herausforderungen. Einerseits wollen die wirtschaftlich stärkeren Mitgliedstaaten ihre Vormachtstellung nicht verlieren und andererseits muss eine Rechtsgrundlage für den gemeinsamen Markt geschaffen werden, welche für alle Markteilnehmer gleichermaßen gilt. Diesem Grundsatz entsprechend ist Rechtsangleichung notwendig um eine Wettbewerbsverzerrung zu vermeiden. Beispielsweise wären unterschiedliche Umweltschutzauflagen innerhalb des gemeinsamen Binnenmarktes, welche Folgen auf Produktionskosten haben können, als wettbewerbsverzerrend anzusehen.

Folgend ist ein wichtiger Aspekt für einen funktionierenden Binnenmarkt eine Harmonisierung des Rechts (Rechtsangleichung in allen Mitgliedstaaten) und ein gemeinsamer Markt ohne innerstaatliche Grenzen. Rechtlich bedeutet dies die Gewährleistung der vier Grundfreiheiten, der Freiheit des Warenverkehrs (Art. 28 bis Art. 37 AEUV), der Freiheit des Personenverkehrs (bestehend aus der Arbeitnehmerfreizügigkeit (Art. 45 bis Art. 48 AEUV) und der Niederlassungsfreiheit für Selbständige (Art. 49 bis Art. 54 AEUV)), der Freiheit des Dienstleistungsverkehrs (Art. 56 bis Art. 62 AEUV) und der Freiheit des Kapitalverkehrs (Art. 63 bis Art. 66 AEUV). Damit die Funktion der Freiheiten gewährleistet werden kann, werden die vier Grundfreiheiten noch durch eine weitere Freiheit ergänzt, nämlich der Freiheit des Zahlungsverkehrs (Art. 63 Abs. 2 AEUV).[12]

[12] *Aicher*, Grundsätze und Ziele des Binnenmarktes, Grundlagen der Rechtsangleichung (2018) 3f.

Dieses Binnenmarktkonzept ist in Art. 3 Abs. 3 EUV wie folgt europarechtlich festgehalten:
„Die Union errichtet einen Binnenmarkt. Sie wirkt auf die nachhaltige Entwicklung Europas auf der Grundlage eines ausgewogenen Wirtschaftswachstums und von Preisstabilität, eine in hohem Maße wettbewerbsfähige soziale Marktwirtschaft, die auf Vollbeschäftigung und sozialen Fortschritt abzielt, sowie ein hohes Maß an Umweltschutz und Verbesserung der Umweltqualität hin. Sie fördert den wissenschaftlichen und technischen Fortschritt.“[13]

Im europäischen Primärrecht regelt auch noch Art. 26 AEUV Bestimmungen zum Binnenmarkt:
„Der Binnenmarkt umfasst einen Raum ohne Binnengrenzen, in dem der freie Verkehr von Waren, Personen, Dienstleistungen und Kapital gemäß den Bestimmungen der Verträge gewährleistet ist.“[14]

Angesichts dieser primärrechtlichen Bestimmungen des Binnenmarktkonzepts im EUV und AEUV bekennt sich die Union dazu, den „wirtschaftlichen und technischen Fortschritt“[15] zu fördern. Inwieweit diese Förderung des technischen Fortschritts auch die Schaffung eines digitalen Binnenmarktes beinhaltet, geht aus diesen allgemein gehaltenen Bestimmungen nicht näher hervor. Der rasante digitale Fortschritt fordert ein geändertes Verständnis der Grundfreiheiten und eröffnet der EU dadurch neue Chancen seine Wettbewerbsfähigkeit zu steigern. Die Aufgabe der EU ist es demzufolge, die Marktteilnehmer zu schützen und ihnen durch angemessene Gesetzesinitiativen Rechtssicherheit auf dem digitalen Binnenmarkt zu geben.

Die Europäische Kommission ging im Mai 2015 durch die Realisierung eines digitalen Binnenmarkts von einem zusätzlichen Wirtschaftsvolumen von 415 Milliarden Euro in der EU aus. An diesen Zahlen lässt sich das durch die Digitalisierung mögliche Potential für die EU gut abschätzen und verdeutlicht nochmals die Bedeutung dieser vierten industriellen Revolution.[16] Seit der Vorstellung der „Strategie für einen digitalen Binnenmarkt“ durch die Europäische Kommission im Jahr 2015 wurden bis jetzt bereits 28 Gesetzesinitiativen beschlossen und zwei weitere befinden sich noch in Begutachtung. In Zusammenhang mit

[13] Art. 3 Abs. 3 EUV
[14] Art. 26 AEUV
[15] Art. 3 Abs. 3 EUV
[16] *Europäische Kommission*, Factsheets: Warum wir einen digitalen Binnenmarkt brauchen (2015) 1-3.

Industrie 4.0-Anwendungen ist vor allem die 3. Säule dieser Strategie „Schaffung einer europäischen digitalen Wirtschaft und digitalen Gesellschaft mit Wachstumspotenzial“ vorrangig zu betrachten.[17]

Aus diesem Schwerpunkt der digitalen Strategie sind für den digitalen Binnenmarkt bereits einige Verordnungen bzw. Richtlinien seit dem Jahr 2015 beschlossen worden.

Folgend eine Übersicht[18] der für das IT-Recht relevanten Normen:

- Verordnung (EU) 2017/1128 des Europäischen Parlaments und des Rates vom 14.Juni 2017 zur grenzüberschreitenden Portabilität von Online-Inhaltediensten im Binnenmarkt[19]
- Verordnung (EU) 2018/302 des Europäischen Parlaments und des Rates vom 28. Februar 2018 über Maßnahmen gegen ungerechtfertigtes Geoblocking und andere Formen der Diskriminierung aufgrund der Staatsangehörigkeit, des Wohnsitzes oder des Ortes der Niederlassung des Kunden innerhalb des Binnenmarkts und zur Änderung der Verordnungen (EG) Nr. 2006/2004 und (EU) 2017/2394 sowie der Richtlinie 2009/22/EG[20]
- Richtlinie (EU) 2018/1808 des Europäischen Parlaments und des Rates vom 14. November 2018 zur Änderung der Richtlinie 2010/13/EU zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung audiovisueller Mediendienste (Richtlinie über audiovisuelle Mediendienste) im Hinblick auf sich verändernde Marktgegebenheiten[21]
- Richtlinie (EU) 2019/770 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen[22]
- Richtlinie (EU) 2019/790 des Europäischen Parlaments und des Rates vom 17. April 2019 über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt und zur Änderung der Richtlinien 96/9/EG und 2001/29/EG[23]

[17] *Europäische Kommission*, Factsheets: Ein digitaler Binnenmarkt zum Nutzen aller Europäer (2019) 1-4.
[18] *Staudegger*, jusIT 2019, 1.
[19] PortabilitätsVO 2017/1128 ABI L 2017/168, 1.
[20] GeoblockingVO 2018/302 ABI L 2018/60 I, 1.
[21] AudiovisuelleMediendiensteRL 2018/1808 ABI L 2018/303, 69.
[22] DigitaleInhalteRL 2019/770 ABI L 2019/136, 1.
[23] UrheberrechtsRL 2019/790 ABI L 2019/130, 92.

- Verordnung (EU) 2018/1807 des Europäischen Parlaments und des Rates vom 14. November 2018 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union[24]
- Richtlinie (EU) 2019/789 des Europäischen Parlaments und des Rates vom 17. April 2019 mit Vorschriften für die Ausübung von Urheberrechten und verwandten Schutzrechten in Bezug auf bestimmte Online-Übertragungen von Sendeunternehmen und die Weiterverbreitung von Fernseh- und Hörfunkprogrammen und zur Änderung der Richtlinie 93/83/EWG des Rates[25]
- Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors[26]
- Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)[27]

Im Folgenden werden die wichtigsten Verordnungen und Richtlinien im Zusammenhang mit Industrie 4.0-Anwendungen analysiert.

Interessant wird zukünftig auch zu beobachten sein, inwieweit eine mögliche horizontale Harmonisierung der Rechtsnormen für den digitalen Binnenmarkt stattfinden wird. Zahlreiche Richtlinien definieren bereits allgemeine Sicherheitsanforderungen für bestimmte Produktgruppen und basierend auf diesen Richtlinien legen die europäischen Normungsorganisationen fest, wie diese Richtlinien-Anforderungen (technisch) erreicht bzw. erfüllt werden können. Es findet somit eine Standardisierung nach definierten Sicherheitsmaßstäben statt.

Im Bereich Industrie 4.0 beschäftigen sich internationale Arbeitsgruppen mit der Erstellung von Normen und Standards. In Österreich arbeitet „Austrian Standards“[28] sehr eng mit dem

[24] FreierDatenverkehrVO 2018/1807 ABI L 2018/303, 59.
[25] UrheberrechtsRL 2019/789 ABI L 2019/130, 82.
[26] OffeneDatenRL 2019/1024 ABI L 2019/172, 56.
[27] Datenschutz-GrundVO 2016/679 ABI L 2016/119, 1.
[28] Austrian Standards ist eine unabhängige Plattform bzw. ein Normungsinstitut, das sich aus Experten diverser Branchen zusammensetzt und Normen bzw. Standards mitentwickelt.

Europäischen Komitee für Normung CEN zusammen. Die Anwendung von Normen und Standards ist grundsätzlich freiwillig und somit nicht unmittelbar rechtsverbindlich. Sind Normen jedoch Vertragsbestandteil oder verweisen EU-Richtlinien auf Normen, so können diese in einem Gerichtsverfahren als Grundlage herangezogen werden. Zusätzlich erleichtert es dem Gericht festzustellen, ob die gültigen Regeln der Technik eingehalten wurden. Vor allem bei Produkthaftungsfragen wird sehr oft auf die Einhaltung von Normen und Standards verwiesen.

Folgend ist es auch im Bereich der Digitalisierung notwendig und wichtig diese Standardisierung mit der Einführung von Normen voranzutreiben.

Die grenzüberschreitende Vernetzung und Interoperabilität von Systemen, die einheitliche Kommunikation (Protokolle, Sicherheitsstandards) und einheitliche Technologien für den Datenaustausch ermöglichen Unternehmen die Wettbewerbsfähigkeit zu steigern. Es ist auch unbestritten, dass durch die Integration von Forschung & Entwicklung eine beschleunigte Weiterentwicklung von Produkten erreicht werden kann.

Weiters stellen Normen die Grundlage für Zertifizierungsprozesse dar, was wiederum Verbrauchern erleichtert festzustellen, ob das Produkt sicherheitsrelevanten Standards entspricht und mit anderen Komponenten kompatibel ist.[29]

## *3.2 Kartellrechtliche Herausforderungen im digitalen Binnenmarkt*

Grenzüberschreitende Vernetzung von Unternehmen, die Anforderungen der Interoperabilität von Systemen, der Zugriff auf und die Verfügbarkeit von großen Datenmengen (Big Data) eröffnen Unternehmen Chancen und ganz neue Möglichkeiten sich am Markt zu positionieren. Dieses Modell der Vernetzung birgt jedoch auch eine große Gefahr dahingehend in sich, dass Unternehmen dazu verleitet werden, diese stärkere Marktposition, welche dadurch möglicherweise erlangt wird, missbräuchlich einzusetzen.

Nachfolgend sollen die möglichen Hausforderungen des digitalen Binnenmarktes und dem Kartell- und Wettbewerbsrecht etwas genauer betrachtet werden.

[29] https://www.austrian-standards.at/infopedia-themencenter/infopedia-artikel/internet-der-dinge-iot/

Die grundlegende Funktion des europäischen bzw. des nationalen Kartellrechts ist die Kontrolle des Verhaltens von Unternehmen auf einem Markt. Ein wesentlicher Grundsatz ist das Selbstständigkeitspostulat, d.h. Unternehmen müssen sich eigenständig verhalten und eine Koordination mit anderen ist nicht erlaubt. Der Gedanke dahinter ist die eigentliche Binnenmarkt-Idee, Wettbewerb auf dem gemeinsamen Markt zu ermöglichen. Durch Wettbewerb können bessere Preise für Kunden erzielt werden und Unternehmen sind gezwungen innovativ und zukunftsorientiert zu agieren. Ein fairer Wettbewerb reguliert den Markt von selbst und stellt noch dazu die Basis für einen funktionierenden Konsumentenschutz sicher. Auf einigen Märkten ist Wettbewerb nicht mehr vorhanden bzw. nur sehr eingeschränkt (Marktmacht[30]), was wiederum zur Konsequenz hat, dass eine unausgewogene Verhandlungssituation entsteht, es keinen Entscheidungsspielraum (keine Auswahlmöglichkeiten) für Konsumenten gibt, höhere Preise verlangt werden (höherer gewinnmaximierender Preis als bei gleichen Wettbewerbsbedingungen), die Geschäftsbedingungen schlechter sind, weniger produziert wird und es allgemein eine Einschränkung der Verbraucherwohlfahrt bzw. Gesamtwohlfahrt gibt.

### 3.2.1 Anwendungsbereich des europäischen Primärrechts

Im Primärrecht ist die Regelung betreffend Wettbewerb in Art. 101 AEUV vereinbart:
„(1) Mit dem Binnenmarkt unvereinbar und verboten sind alle Vereinbarungen zwischen Unternehmen, Beschlüsse von Unternehmensvereinigungen und aufeinander abgestimmte Verhaltensweisen, welche den Handel zwischen Mitgliedstaaten zu beeinträchtigen geeignet sind und eine Verhinderung, Einschränkung oder Verfälschung des Wettbewerbs innerhalb des Binnenmarkts bezwecken oder bewirken, insbesondere [ …]
(3) Die Bestimmungen des Absatzes 1 können für nicht anwendbar erklärt werden auf

- Vereinbarungen oder Gruppen von Vereinbarungen zwischen Unternehmen,
- Beschlüsse oder Gruppen von Beschlüssen von Unternehmensvereinigungen,
- aufeinander abgestimmte Verhaltensweisen oder Gruppen von solchen,

die unter angemessener Beteiligung der Verbraucher an dem entstehenden Gewinn zur Verbesserung der Warenerzeugung oder -verteilung oder zur Förderung des technischen oder wirtschaftlichen Fortschritts beitragen, ohne dass den beteiligten Unternehmen

[30] Marktmacht bedeutet, dass ein Unternehmen durch eine beherrschende Stellung auf einem Markt eine wirtschaftliche Machtstellung gegenüber anderen Marktteilnehmern erhält.

a) Beschränkungen auferlegt werden, die für die Verwirklichung dieser Ziele nicht unerlässlich sind, oder

b) Möglichkeiten eröffnet werden, für einen wesentlichen Teil der betreffenden Waren den Wettbewerb auszuschalten."[31]

Wesentlich für jeden Vertrag zwischen Unternehmen ist daher die Einhaltung der kartell- und wettbewerbsrechtlichen Vorgaben. Diese Bestimmungen sind sowohl auf vertikale Verträge (vom Ursprung der Wertschöpfungskette bis zum Kunden - d.h. jeden Bezugsvertrag) als auch auf jegliche Unternehmenszusammenschluss-Verträge (M&A; JointVenture; Vereinbarungen) anwendbar und werden bei einem Kartellverstoß als nichtig erklärt. Bei der Prüfung der Tatbestandsmerkmale „Verhinderung, Einschränkung oder Verfälschung des Wettbewerbs"[32] ist der Adressat von Art. 101 AEUV das Unternehmen. Das nationale Kartellrecht und das Europarecht kommen kumulativ zur Anwendung. National dürfen strengere Missbrauchsregulierungen festgelegt werden. Bei einer Verfahrenseinleitung durch die Europäische Kommission entfällt die Zuständigkeit der Wettbewerbsbehörde der Mitgliedstaaten. Bei der Prüfung wird nach der Feststellung der Anwendbarkeit von Art. 101 Abs. 1 AEUV insbesondere die Spürbarkeit der Wettbewerbsbeschränkung geprüft. Hierzu gibt es Marktanteil-Schwellenwerte, welche für die Feststellung von horizontalen sowie von vertikalen „Kooperationen" herangezogen werden. Auf diese detaillierten Schwellenwert-Regulierungen wird im Rahmen dieser Master Thesis nicht näher eingegangen.

Der zunehmende Druck am Markt macht es für Unternehmen ohne äußere Unterstützung (Kooperationen) und häufig aufgrund von mangelnden qualifizierten Ressourcen und fehlenden finanziellen Mitteln vor allem für die kleinen und mittleren Unternehmen (KMUs) äußerst schwierig konkurrenzfähig zu bleiben.

Das *Institut der deutschen Wirtschaft Köln*[33] hat im Rahmen eines Forschungsprojekts die kartellrechtlichen Herausforderungen bei der Implementierung von Industrie 4.0-Anwendungen näher untersucht. Es wurde festgestellt, dass sich Unternehmen durch Vernetzung, Austausch und Analyse von Daten oder dem Einsatz von intelligenten Maschinen

[31] Art. 101 AEUV
[32] Art. 101 Abs. 1 AEUV
[33] *Rusche/Demary*, Zwischen Kooperation und Wettbewerb: Industrie 4.0 und europäisches Kartellrecht IW-Report No. 14/2017, 1ff.

in die Lage versetzen können die Marktmacht zu erreichen und wesentliche Wettbewerbsvorteile gegenüber der Konkurrenz zu erzielen. Eine marktbeherrschende Stellung bzw. die Erlangung der Marktmacht aufgrund des Erfolgs eines Unternehmens oder Produktes per se stellt zwar noch keinen kartellrechtswidrigen Sachverhalt dar, jedoch ist die missbräuchliche Ausnutzung dieser Machtposition gegenüber den anderen Marktteilnehmern rechtswidrig (Art. 102 AEUV). Im Bereich Big Data begründet der Besitz von exklusiven Daten möglicherweise einen wettbewerbsbeschränkenden Sachverhalt, wenn dieser die Machtposition eines Unternehmens stärkt und zum Beispiel erhöhte Preise für Produkte verlangt werden können. Ein einzigartiger Datensatz kann aber auch durch ein Urheberrecht oder Geschäftsgeheimnis geschützt sein. Verhindert ein solches Urheberrecht bzw. die Verweigerung einer Lizenz, z.B. auf eine Industrie 4.0-Anwendung, den Marktzugang für andere Unternehmen, so ist dieses Verhalten unter bestimmten Bedingungen als Missbrauch einer beherrschenden Stellung einzustufen.[34]

### 3.2.2 Rechtssache Microsoft Corp.

In der Rechtssache T-201/04 R, Microsoft Corp. gegen die Europäische Kommission, wurde Microsoft dazu verurteilt, Interoperabilitätsinformationen (u.a. Protokolle für die Kommunikation) seiner Software offenzulegen. In diesem Urteil wird dann von einer missbräuchlichen Stellung ausgegangen, wenn die folgenden drei Bedingungen kumulativ erfüllt sind (man spricht in diesem Fall auch von einem außergewöhnlichen Umstand). Es wird verlangt, dass „das Auftreten eines neuen Produkts verhindert wird, nach dem eine potenzielle Nachfrage der Verbraucher besteht, die missbräuchliche Stellung nicht gerechtfertigt sein darf und diese geeignet sein muss, jeglichen Wettbewerb auf einem abgeleiteten Markt auszuschließen.“[35]

Versuchen wir nun diese drei Bedingungen vergleichend auf die Implementierung einer Industrie 4.0-Lösung anzuwenden und die möglichen rechtlichen Hindernisse zu analysieren.
Damit die Rechtsinterpretation etwas anschaulicher wird, konkretisieren wir es an folgendem fiktivem Beispiel:
Ein Automobilzulieferer betreibt Industrieöfen für das Wärmebehandeln von metallischen Komponenten. Diese Industrieöfen nutzen eine Industrie 4.0-Technologie zur Unterstützung

[34] *Rusche/Demary*, Zwischen Kooperation und Wettbewerb: Industrie 4.0 und europäisches Kartellrecht IW-Report No. 14/2017, 7ff.
[35] EuG 17.9.2007, T-201/04 R, *Microsoft* Rz 330

der Wartung und Instandhaltung der Anlagen, im Speziellen zur Analyse der Ausfallswahrscheinlichkeit von Komponenten, zur Prozessoptimierung und Sicherstellung der Produktqualität durch Reduktion der Anlagenstillstandszeiten. Spezifische Maschinen- und Prozessdaten werden erfasst, ausgewertet und zu Prognose- sowie Optimierungszwecken eingesetzt. Die IIoT-Anwendung welche für die Analyse der Wärmebehandlungsdaten eingesetzt wird, ist ein urheberrechtlich geschütztes Produkt des Industrieofen-Herstellers. Der Automobilzulieferer hat das Nutzungsrecht an dieser IIoT-Anwendung mit dem Industrieofen miterworben. In unserem Beispiel handelt sich um eine Komponente, welche bei der Automobil-Antriebseinheit unbedingt erforderlich ist, um die $CO_2$-Emissionen unter den maximalen gesetzlich festgelegten Limits zu halten.

Der folgende Abschnitt analysiert die Bedingung Nr. 1 („die Weigerung muss das Auftreten eines neuen Produkts verhindern, nach dem eine potenzielle Nachfrage der Verbraucher besteht“[36]) der Rechtssache T-201/04 R im Zusammenhang mit dem skizzierten Beispiel:
Für den Fall der Urteilsinterpretation nehmen wir an, dass es sich hierbei um ein Produkt handelt, nach dem eine potentielle Nachfrage am Markt besteht. Solange das Produkt durch den Einsatz der Industrie 4.0-Technologie am Markt unabhängig agieren kann und das Auftreten eines anderen neuen Produktes nicht verhindert, stellt es unmittelbar kein rechtswidriges Handeln dar. Nimmt die Industrie 4.0-Technologie in der Produktion jedoch so großen Einfluss auf das Produkt, sodass dieser Vorteil andere neue Produkte daran hindert auf den Markt zu gelangen, dann wäre diese erste Bedingung erfüllt. Dies wäre der Fall, wenn durch den Einsatz dieser Industrie 4.0-Technologie der Produktionsprozess so optimiert wird, dass die Komponente ein Alleinstellungsmerkmal aufweist, welches für die Einhaltung der $CO_2$-Grenzwerte unerlässlich ist. D.h. durch die digitale Unterstützung wird der Wettbewerb so stark eingeschränkt, dass diese Komponente ohne die IIoT-Anwendung nicht mehr wettbewerbsfähig angeboten werden kann und so ein Auftreten eines konkurrenzfähigen Produktes am Markt verhindert.

Diese beherrschende Stellung verhindert die Aufrechterhaltung eines wirksamen Wettbewerbs und schafft dem Automobilzulieferer eine Möglichkeit sich seinen Wettbewerbern, seinen Abnehmern, seinen Verbrauchern gegenüber unabhängig zu verhalten. Nichtsdestotrotz muss das Unternehmen nicht ohne Weiteres keine Rücksicht auf andere Wettbewerber, Verbraucher,

[36] EuG 17.9.2007, T-201/04 R, *Microsoft* Rz 330

F&E, Produktqualität, Preis etc. nehmen, wenn die Stellung am Markt, durch den aus eigener Kraft erarbeiteten technischen oder technologischen Vorsprungs, erreicht worden ist.

Für eine spezifische Beurteilung der marktbeherrschenden Stellung müssen auch die Kriterien Marktanteile, Unternehmensstruktur (technologischer Vorsprung sowie Wirtschafts- und Finanzkraft) und das Marktverhalten (u.a. fehlender Wettbewerbsdruck) bewertet werden.

Der folgende Abschnitt analysiert die Bedingung Nr. 2 („die Weigerung darf nicht gerechtfertigt sein“[37]) der Rechtssache T-201/04 R im Zusammenhang mit dem skizzierten Beispiel:
Die Entwicklung und der Einsatz dieser Industrie 4.0-Technologie hat es dem Automobilzulieferer ermöglicht eine beherrschende Stellung mit einem Produkt zu erlangen. Diese beherrschende Stellung am Markt ist folgend durch den technologischen Fortschritt erlangt worden, welcher auf die Industrie 4.0-Anwendung zurückzuführen ist. Rechtlich relevant ist nun, ob der Einsatz dieser Industrie 4.0-Anwendung objektiv gerechtfertigt ist oder nicht. Einerseits ist die Maßnahme aus Sicht des Automobilzulieferers, welcher Investitionen in die Industrie 4.0-Technologie getätigt hat, gerechtfertigt und stellt kein missbräuchliches Verhalten dar.

Andererseits führt die Verhaltensweise des Unternehmens zu einem geschwächten Wettbewerb. Dieser wird durch die Verwendung von Mitteln geschwächt, die von einem normalen Produkt- oder Dienstleistungswettbewerb auf der Grundlage der Leistungen und eingesetzten Mittel der Marktteilnehmer abweicht. Das Konkurrieren nur mit der eigenen Leistung ist zwar zulässig, jedoch nicht wenn man zu Mitteln greift, welche mit dem eigenen Produkt nichts zu tun haben. Einerseits werden Eigenschaften und Verhaltensweisen von Komponenten mittels Daten für die Weiterentwicklung herangezogen, welche indirekt mit dem Produkt zu tun haben, anderseits handelt es sich bei der Industrie 4.0-Technologie um ein vom Produkt entkoppeltes selbstständig durch vorgegebene Algorithmen agierendes System.

Im Sinne der Weiterentwicklung des Produktes und des positiven Beitrags für die Gesellschaft bzw. zum Umweltschutz ($CO_2$-Reduktion) ist der Einsatz der Industrie 4.0-Technologie unter Berücksichtigung der eingeschränkten objektiv genannten Erwägungen durchaus als sachlich

[37] EuG 17.9.2007, T-201/04 R, *Microsoft* Rz 330

gerechtfertigte Maßnahme anzusehen. Inwieweit die Maßnahme eine nicht gerechtfertigte Benachteiligung der Wettbewerber zur Folge hat, muss gesondert beurteilt und im Einzelfall geprüft werden.

Der folgende Abschnitt analysiert die Bedingung Nr. 3 („die Weigerung muss geeignet sein, jeglichen Wettbewerb auf einem abgeleiteten Markt auszuschließen“[38]) der Rechtssache T-201/04 R im Zusammenhang mit dem skizzierten Beispiel:
Nachdem in unserem fiktiven Beispiel nur mit dieser einen Komponente die Erreichung der gesetzlichen $CO_2$-Auflagen erreicht werden kann, ist es als eine Maßnahme gleicher Wirkung, wie eine Alleinbezugsverpflichtung anzusehen. Dadurch, dass das Produkt durch den Einsatz der Industrie 4.0-Anwendung ein Alleinstellungsmerkmal kreiert und so ein neuer Markt entsteht, ist dieses Produkt geeignet, um jeglichen Wettbewerb auf diesem Markt auszuschließen. Die durch den Wettbewerb am Markt platzierten Komponenten werden folglich irrelevant für die Abnehmer, da mit diesen die gesetzlich geforderten $CO_2$-Werte nicht erreicht werden können.

Damit die konstruierte beherrschende Stellung nicht missbräuchlich verwendet und Wettbewerb auf diesem Markt ermöglicht wird, könnte die Offenlegung der Industrie 4.0-Anwendung gefordert werden. Im Unterschied zum analysierten Urteil der Rechtssache T-201/04 R differenziert sich der Sachverhalt des Beispiels dahingehend, dass mehrere Parteien involviert sind. Der Automobilzulieferer einerseits, welcher das finale Produkt und die Daten zur Analyse bereitstellt und der Industrieofen-Hersteller auf der anderen Seite, welcher mittels Industrie 4.0-Anwendung diesen Entwicklungsvorsprung erst ermöglicht. Für die Erreichung der beherrschenden Stellung war demzufolge eine zweite Partei ausschlaggebend. Es ist davon auszugehen, dass es ohne eine objektive sachliche Rechtfertigung schwierig wird eine Lizenzverweigerung an Immaterialgüterrechten (z.B. an dieser Industrie 4.0-Technologie) wirksam durchzusetzen. In diesem Sachverhalt unberücksichtigt sind möglicherweise abgeschlossene Verträge zwischen den beiden Unternehmen, welche Ausschließlichkeitsrechte an der eingesetzten Industrie 4.0-Technologie, das Dateneigentum bzw. die Verwertung oder Weitergabe der Daten und Analyseergebnisse an Dritte regeln könnten. Dieses Beispiel macht deutlich, wie wichtig die detaillierte wettbewerbs- und

[38] EuG 17.9.2007, T-201/04 R, *Microsoft* Rz 330

kartellrechtliche Betrachtung in Verträgen ist, in welchen digitale Produkte sowie datenbasierende Kooperationen eine Rolle spielen.

Die dargestellten Interpretationen rechtfertigen die Aussage, dass das Missbrauchsverbot, d.h. die Kontrolle des Verhaltens eines oder mehrerer Unternehmen auf dem Markt, auch für den digitalen Binnenmarkt und im Speziellen für Industrie 4.0-Anwendungen Gültigkeit hat.

In der Rechtssache T-201/04 R beruft man sich auf den Art. 102 AEUV und dem Missbrauch einer marktbeherrschenden Stellung. Der Art. 102 AEUV regelt das Verbot einer missbräuchlichen Stellung und die Folgen des Missbrauchs wie folgt:
„Mit dem Binnenmarkt unvereinbar und verboten ist die missbräuchliche Ausnutzung einer beherrschenden Stellung auf dem Binnenmarkt oder auf einem wesentlichen Teil desselben durch ein oder mehrere Unternehmen, soweit dies dazu führen kann, den Handel zwischen Mitgliedstaaten zu beeinträchtigen.
Dieser Missbrauch kann insbesondere in Folgendem bestehen:

> a) der unmittelbaren oder mittelbaren Erzwingung von unangemessenen Einkaufs- oder Verkaufspreisen oder sonstigen Geschäftsbedingungen;
> b) der Einschränkung der Erzeugung, des Absatzes oder der technischen Entwicklung zum Schaden der Verbraucher;
> c) der Anwendung unterschiedlicher Bedingungen bei gleichwertigen Leistungen gegenüber Handelspartnern, wodurch diese im Wettbewerb benachteiligt werden;
> d) der an den Abschluss von Verträgen geknüpften Bedingung, dass die Vertragspartner zusätzliche Leistungen annehmen, die weder sachlich noch nach Handelsbrauch in Beziehung zum Vertragsgegenstand stehen.“[39]

Europarechtlich sind somit auch für den digitalen Binnenmarkt die drei materiell rechtlichen Säulen des Wettbewerbs- und Kartellrechts relevant. Diese sind definiert durch den Art. 101 AEUV sowie den Gruppenfreistellungsverordnungen (GVO's), dem Art. 102 AEUV und der Fusionskontrollverordnung (FKVO).

Der Art. 101 Abs. 3 AEUV begründet eine Ausnahme. Art. 101 Abs. 3 wird in der Form angewendet, dass die Europäische Kommission eine Verordnung erlässt (GVO -

[39] Art. 102 AEUV

Gruppenfreistellungsverordnung) wonach das Kartellverbot keine Anwendung findet, wenn der Vertrag in den Anwendungsbereich dieser GVO fällt.

Unter Anwendung von Art. 101 Abs. 3 AEUV (Ausnahmetatbestand) und der F&E Gruppenfreistellungsverordnung VO (EU) Nr. 1217/2010[40] stellt die Regelung, unter bestimmten Bedingungen im Kartellrecht eine rechtmäßige Möglichkeit zur Realisierung von F&E-Kooperationen dar. Für eine gemeinsame Datenverarbeitung durch zwei oder mehrere Unternehmen zu F&E-Zwecken (z.B.: Optimierung des Produktionsprozesses, Kosteneinsparungen, Produktentwicklung) ist die Weitergabe von „Know-how" (Kenntnisse, die für Herstellung von Produkten bedeutsam und nützlich sind) entscheidend für die Anwendung der F&E GVO. Es ist anzunehmen, dass durch die gemeinsame Verarbeitung von Daten eine Verbesserung des Produktes zu erwarten ist, womit diese Verwertung in den Anwendungsbereich der Verordnung fällt.[41] Diese Ausnahmeregelung ermöglicht es Unternehmen im Rahmen von gemeinsamen F&E-Projekten wertvolle Daten miteinander auszutauschen und diese für die Weiterentwicklung der Produkte einzusetzen.
Bevor eine Beurteilung im Sinne der zuvor genannten primärrechtlichen Rechtsgrundlagen überhaupt durchgeführt werden kann, ist auf jeden Fall eine individuelle Marktbeurteilung erforderlich (Marktabgrenzung und Beurteilung des Marktanteils).

Bei der Marktbeurteilung kommt es vorrangig auf die Sicht der Nachfrager an, welche nach dem Grundsatz der Substituierbarkeit der Nachfrage beurteilt werden. Folgende Kriterien werden für die Prüfung der Substituierbarkeit von Waren und Dienstleistungen herangezogen: Bedürfnis, Qualität, Preis, Eigenschaft, Funktion und Verwendungszweck.

Bei Industrie 4.0-Anwendungen könnten im Gegensatz zu physischen Waren die Kriterien Messgröße, Abtastfrequenz, Messbereich, Verfahren, Datenverarbeitung, Zugriffsrechte, Datensicherheit, Dateninterpretation, Kompatibilität mit anderen Systemen, Datenübertragung, Zykluszeit, Reichweite o.Ä. für die sachliche Beurteilung berücksichtigt werden. Ergänzend zur sachlichen Marktabgrenzung muss auch die räumliche Komponente bestimmt werden. Hierzu wird der räumlich relevante Markt in dem hinreichend homogene

[40] Verordnung (EU) Nr. 1217/2010 der Kommission vom 14. Dezember 2010 über die Anwendung von Artikel 101 Absatz 3 des Vertrags über die Arbeitsweise der Europäischen Union auf bestimmte Gruppen von Vereinbarungen über Forschung und Entwicklung ABI L 2010/335, 36.
[41] *Ensthaler*, NJW 2016, 8f.

Wettbewerbsbedingungen herrschen, welche sich von den angrenzenden Märkten unterscheiden, für die Bewertung herangezogen.[42]

Eine Marktabgrenzung im digitalen Raum durchzuführen ist insofern eine Herausforderung, als zumeist keine physischen Waren beurteilt werden und sich die Situationen oft nicht eindeutig räumlich zuordnen lassen, da bei Industrie 4.0-Anwendungen von einer Vernetzung von Maschinen und Anlagen ausgegangen werden kann.[43]

### 3.2.3 Anwendungsbereich Condition Monitoring

Basierend auf den genannten Rechtsgrundlagen betrachten wir am Beispiel einer Instandhaltungsanwendung (in unserem Beispiel „Condition Monitoring“) den Zusammenhang zwischen einer Industrie 4.0-Anwendung und dem Kartellrecht.

Wie in Kapitel 3.2 dieser Master Thesis beschrieben, werden mittels Condition Monitoring in Echtzeit Anlagenzustände, welche von Sensoren und Aktoren erfasst und übertragen werden, gespeichert, aufgezeichnet und dokumentiert. Üblicherweise handelt es ich hierbei um Maschinen- oder Prozessdaten, welche nach einer Analyse dazu genutzt werden, den Gesundheitszustand einer Maschine oder Anlage zu beurteilen (u.a. aufgrund von Trends oder Erfahrungswerten), um basierend auf diesen Erkenntnissen geeignete Instandhaltungsmaßnahmen festzulegen. Mögliche Ergebnisse und Maßnahmen sind u.a. Lebensdauerbeurteilungen von Komponenten, Festlegung von Instandhaltungsintervallen oder Maßnahmen zur Prozessoptimierung. Maschinen und Anlagen können dadurch sicherer gemacht, der Instandhaltungsaufwand sowie Anlagen-Stillstandszeiten können reduziert und die Produktivität gesteigert werden.

Betrachtet man Condition Monitoring isoliert von den weiteren am Markt verfügbaren Instandhaltungsmöglichkeiten, die man noch kombinieren könnte, so unterliegt dieses Tool im Allgemeinen keinen automatisierten Nachbestellungen von Komponenten (d.h. automatisierte

[42] *Europäische Kommission*, Bekanntmachung der Kommission über die Definition des relevanten Marktes im Sinne des Wettbewerbsrechts der Gemeinschaft (97/C 372/03) ABI C 1997/372, 5.
[43] *Bundesministerium für Wirtschaft und Energie (BMWi)*, Industrie 4.0 – Kartellrechtliche Betrachtungen (2018) 5ff.

vertikale Verträge mit Lieferanten). In der nachfolgenden Betrachtung wird diese automatisierte Ausführung von Aktionen deshalb auch nicht weiter berücksichtigt.

Inwieweit der Einsatz von Condition Monitoring, wie zuvor beschrieben, ausreicht um als Unternehmen eine beherrschende Stellung zu erreichen, ist äußerst fraglich und muss im Einzelfall im Detail betrachtet und beurteilt werden. Rechtlich ist es unerheblich wie man die marktbeherrschende Stellung erreicht. Wenn ein Unternehmen die marktbeherrschende Stellung aufgrund des technologischen Vorsprungs durch Condition Monitoring erreicht und dadurch günstiger und besser anbieten kann, dann ist das grundsätzlich nach Art. 102 AEUV nicht verboten, sofern diese beherrschende Stellung nicht missbräuchlich verwendet wird. Die Einzigartigkeit als eine wesentliche Eigenschaft von Daten und die Eigentumsfrage an Daten als möglicher Schranken für einen potentiellen Marktzutritt werden die Kartellbehörden zukünftig beschäftigen.[44] Die Fragen zur Datenhoheit und den rechtlichen Mitteln werden im Kapitel 5.2 dieser Master Thesis behandelt.

## *3.3 Ausblick Kartell- und Wettbewerbsrecht*

Der sehr dynamische Markt und die zunehmenden digitalen Anwendungen mit einem kurzen Produktlebenszyklus lassen erwarten, dass es durch den intransparenten Datenverkehr, der steigenden Anzahl an Kooperationen durch Vernetzung und durch die folgend rasch ändernden Markt- und Wettbewerbsverhältnisse zu kritischen kartell- und wettbewerbsrechtlichen Situationen kommen wird. Vor allem KMU's erwarten sich durch unternehmensübergreifende F&E-Aktivitäten und engere Vernetzung mit anderen Unternehmen kürzere Produktentwicklungszeiten, innovative Produkte und niedrigere Kosten aufgrund von Kosten- und Ressourcen-Sharing sowie Nutzung gemeinsamer Plattformen innerhalb der Kooperationen.

Interessant wird zu beobachten sein, wie rasch die Verfahren durch Kartellbehörden eingeleitet und durchgeführt werden können. Durch die unkontrollierte Geschwindigkeit der Märkte ist der Anspruch an die Reaktionsgeschwindigkeit der Behörden sehr hoch, um rechtzeitig korrigierende Maßnahmen für die Wiederherstellung von fairen Wettbewerbsverhältnissen

[44] *Bundesministerium für Wirtschaft und Energie (BMWi)*, Industrie 4.0 – Kartellrechtliche Betrachtungen (2018) 12f.

einzuleiten. In der kartellrechtlichen Betrachtung von Industrie 4.0, erstellt durch das deutsche *Bundesministerium für Wirtschaft und Energie (BMWi)*, wird davon ausgegangen, dass die Maßnahmen der Kartellbehörden mit der derzeitigen Ausrichtung für die neuen digitalen Herausforderungen zu träge sind und auch die Auswirkung von kurzfristigen einstweiligen Aktionen auf den Markt bzw. Wettbewerb nicht vorhersehbar ist. Zweckmäßig ist es aus Sicht des *BMWi* jedenfalls, die aktuellen Regelwerke, hier allen voran die nationalen Wettbewerbsregeln und die europarechtlichen GVO's, zu überarbeiten bzw. zu erweitern und an die Herausforderungen des digitalen Zeitalters anzupassen. Um eine geordnete und transparente Vernetzung zwischen Unternehmen sowie Produktionsprozessen zu ermöglichen und spezifischen Lösungen vorzubeugen, schlägt die Monopolkommission vor, Standards und einheitliche Rahmenbedingungen für den Datenaustausch zu schaffen und den Markt ständig und genauer zu beobachten. Individuelle digitale Produkte und Anwendungen sind mit dem Risiko verbunden, dass Abnehmer an diese Produkte (u.a. aufgrund von mangelnden Alternativen) gebunden sind (Lock-in-Effekte) und so eine unausgewogene und verfälschte Wettbewerbssituation entsteht.[45] Ergänzend soll eine kurze Reaktionsgeschwindigkeit der Kartellbehörden durch aktuell verfügbare empirische Untersuchungen des Marktes erreicht werden, um bei Bedarf auf den Markt abgestimmte Abschreckungsmaßnahmen umgehend einzuleiten.[46]

Es kann erwartet werden, dass die Entwicklung und Umsetzung von internationalen Standards und Normen für Industrie 4.0-Technologien sowohl einen positiven Effekt auf die Entwicklung des Marktes und auf einen gesunden Wettbewerb haben, als auch auf die Förderung von Innovationen Einfluss nehmen.

[45] *Monopolkommission*, SG 68: Wettbewerbspolitik: Herausforderung digitale Märkte (2015) 186f.
[46] *Bundesministerium für Wirtschaft und Energie (BMWi),* Industrie 4.0 – Kartellrechtliche Betrachtungen (2018) 13f.

# 4 Rechtsfragen für digitale Anwendungen / Serviceleistungen

Die einführenden Betrachtungen in den vorhergehenden Kapiteln haben gezeigt, wie präsent und komplex die rechtlichen Themen durch die Digitalisierung geworden sind. Einen ganz wesentlichen Bestandteil im digitalen Raum nehmen vor allem die Daten, durch die rapide Vernetzung innerhalb der Gesellschaft, ein. Diese haben sich zunehmend zu einem wirtschaftlich sehr bedeutenden Gut entwickelt.

Dieser Abschnitt widmet sich deshalb dem Datenverkehr sowie der Untersuchung und rechtlichen Bewertung der daraus resultierenden Rechtsfragen rund um digitale Anwendungen bzw. Serviceleistungen (Dienstleistungen) wie Condition Monitoring und Cloud-Computing.

## *4.1 Datenverkehr – der Datenbegriff*

Die globale Vernetzung spielt nicht nur im privaten Umfeld durch Internet und Social Media eine bedeutende und in vielen Bereichen nicht mehr wegzudenkende Rolle, sondern hat auch in Produktionsanlagen („smart factories“) Einzug gehalten. Das Internet der Dinge ist mittlerweile sehr weitreichend in der Gesellschaft angekommen und vernetzt neben Dingen in Häusern („smart home“) auch Autos („connected cars“) und andere Alltagsgegenstände. Die Kommunikation zwischen den einzelnen Dingen funktioniert zumeist in Echtzeit, automatisch und unbemerkt im Hintergrund, ohne aktives Zutun einer natürlichen oder juristischen Person. Im Wesentlichen werden bei diesen Kommunikations-Aktivitäten, Informationen und Daten über eine definierte Schnittstelle erfasst, ausgetauscht und gespeichert. Hierbei können sowohl personenbezogene- als auch nicht-personenbezogene Daten übertragen werden.[47]

Bevor wir die rechtlichen Aspekte in diese Betrachtung miteinbeziehen, versuchen wir zuerst den Begriff „Daten“ abzugrenzen. In der Literatur findet man diverse, oft branchenspezifische, jedoch keine einheitliche Definition des Datenbegriffs.

[47] *Škorjanc,* ipCompetence 2018 H 20, 26.

*Raffling/Schock* definieren in ihrem Praxishandbuch „Digitale Wirtschaft und Industrie 4.0“ den Begriff maschinengenerierter „Daten“ wie folgt:
„Daten sind „zum Zweck der Verarbeitung zusammengefasste Zeichen, die aufgrund bekannter oder unterstellter Abmachungen Informationen (d.h. Angaben über Sachverhalte und Vorgänge) darstellen“ (codierte Information).“[48]

In der internationalen Norm ISO/IEC 2382:2015 werden Daten wie folgt definiert:
„ (…) reinterpretable representation of information […] in a formalized manner suitable for communication, interpretation, or processing. “[49]

Daten sind demnach eine Repräsentation von Informationen in codierter Form, welche auf Basis eines Übereinkommens kommuniziert, interpretiert oder weiterverarbeitet werden. Folglich ist anzunehmen, dass Daten unterschiedlichste Informationen wie z.B. Ort, Datum, Zeit, Messwerte, Maschinen- oder Anlagenzustände, Gesundheitsdaten, Fitnessdaten, etc. beinhalten können, welche dann via Kommunikationsmedien verbreitet und ausgetauscht werden. Von vielen Personen oder Unternehmen wird zumeist nicht bewusst wahrgenommen, welche sensiblen und oftmals persönlichen Daten offengelegt und von anderen weiterverarbeitet werden. Unternehmen gehen den Weg und eignen sich Daten durch Verbraucher-Zustimmung in AGB’s oder auf Basis von Willenserklärungen an. Aufgrund der Komplexität der Datenschutzthematik haben Verbraucher oft keine andere Möglichkeit als diesen Bedingungen zuzustimmen, wenn Sie an einem Kauf bzw. der vollwertigen Nutzung des Produkts interessiert sind. Welche Konsequenzen eine solche Zustimmung für Unternehmen und Verbraucher hat, ist für viele Beteiligte oft nicht offensichtlich.

Im folgenden Abschnitt werden diese skizzierten datenrechtlichen Unklarheiten und europarechtlichen Rahmenbedingungen zusammengefasst und analysiert.

[48] *Raffling/Schock (Hrsg)*, Digitale Wirtschaft und Industrie 4.0 (2018) 84.
[49] *International Organization for Standardization*, ISO/IEC 2382:2015 (E) (2015) 1ff.

## *4.2 Datenhoheit – das Dateneigentum*

Durch die wirtschaftliche Wertigkeit, welche maschinengenerierte Daten aus Industrieanlagen durch die zunehmende Vernetzung vor allem für produzierende Unternehmen erhalten haben, ist die Frage des Dateneigentums eine ganz wesentliche. Fortführend ist zu hinterfragen, wer die Daten und Datenwege kontrolliert? Die Europäische Kommission legt die derzeitige Rechtslage so aus, dass diese Frage weitgehend durch einzelvertragliche Regelungen geregelt wird, mit dem negativen Effekt, dass häufig die schwächere Partei (u.a. KMU's) das Nachsehen bei der Verhandlung der Vertragsbedingungen hat.[50]

Als mögliche alternative Maßnahmen zur Regelung des Dateneigentums werden u.a. „technische Maßnahmen, Modellverträge oder dispositives Vertragsrecht"[51] genannt.

Die Europäische Kommission forciert Regelungen und Maßnahmen zu implementieren, um einen möglichst freien Verkehr von Daten im EU-Binnenmarkt zu gewährleisten und hat hierzu einige Vorstellungen möglicher Umsetzungsideen formuliert. Neben weiteren Überlegungen sind die für Industrie 4.0-Anwendungen bedeutendsten Vorschläge die „Förderung des leichteren Zugangs zu maschinengenerierten Daten als Innovationsquelle; die Schaffung von Anreizen für das Teilen von Daten und der Erarbeitung von Vorschlägen unter Berücksichtigung des geltenden Rechts; der Schutz von Investitionen, welche in die Produktentwicklung getätigt werden; die Vermeidung der Offenlegung von vertraulichen Daten durch Klassifizierung von Daten; die Minimierung von Lock-in-Effekten; die Förderung von Kommunikationsstandards und Normen für die Identifizierung von Datenquellen; die Erarbeitung von Standardvertragsklauseln (Unterstützung von KMU's); die Begründung von Rechten für den „Erzeuger der Daten" und die Schaffung von Zugangsregeln zu Daten gegen Entgelt".[52] Diese vorgeschlagenen Maßnahmen behandeln die aktuell offenen Fragen der verschiedensten involvierten Interessensträger.

Die Massenverarbeitung von Daten und damit verbundenen Sicherheitsfragen sollen weiter durch Förderung der Interoperabilität von Systemen und der Weiterentwicklung von

[50] *Europäische Kommission*, COM(2017) 9 final 12.
[51] *Wiebe*, ecolex 2017, 783ff.
[52] *Europäische Kommission*, COM(2017) 9 final 12f.

spezifischen technischen Normen und Standards für die Übertragung von Daten zukünftig sichergestellt werden.[53]

*Andreas Wiebe* skizziert in seinem ecolex Beitrag „Wem gehören maschinengenerierte Daten?“ ein mögliches Szenario eines europäischen „Datenproduzentenrechts“. In diesem Leistungsschutzrecht für Daten geht man davon aus, dass der Investor (der die Daten schafft; die Anlagen oder Maschinen bereitstellt, o.Ä.) als Daten-Rechteinhaber qualifiziert wird (angelehnt an einen Know-How-Schutz). Im Falle von produzierenden Unternehmen, welche Industrie 4.0-Anwendungen im Einsatz haben, ist anzunehmen, dass der Anlagenbetreiber der rechtliche Inhaber der Daten wäre. Dieser ist generell nicht daran interessiert seine Produktionsdaten außerhalb der Industrie 4.0-Anwendung Wettbewerbern oder anderen Marktteilnehmern offenzulegen. Die Hersteller der Anlagen bzw. die Dienstleister der Industrie 4.0-Anwendungen haben dagegen ein berechtigtes Interesse an den generierten Daten, als Grundlage für eine raschere Weiterentwicklung, sowie im Sinne einer Innovationsförderung ihrer Anlagen und IT-Anwendungen. Die generierten Daten würden im Fall des Beispiels von Herrn *Wiebe* nur intern ausgetauscht werden und würden von der Offenlegung zu externen Dritten geschützt und nur unter bestimmten Bedingungen und in beschränktem Umfang zugänglich gemacht werden (mögliche Ausnahmen wären: Produktverbesserungen, öffentliches Interesse oder F&E). Der Daten-Rechteinhaber besitzt somit auch keine Exklusivrechte an den Daten. Im Unterschied zum Datenbankschutzrecht (Richtlinie 96/9/EG) wären in diesem Leistungsschutzrecht auch die Daten selbst geschützt und nicht nur die Datenbank.[54] Es wird gewissermaßen eine Kategorisierung der Daten vergleichbar mit dem Vorschlag der Europäischen Kommission vorgenommen. Hinsichtlich der tatsächlichen Umsetzbarkeit dieses Vorschlags, insbesondere der klaren Trennung von Daten, der individuellen Rechtevergabe und der gerechten Preisfindung für den Wert der Daten, begegnen die Beteiligten mit Skepsis.[55]

[53] *Europäische Kommission*, COM(2017) 9 final 18f.
[54] *Ensthaler*, NJW 2016, 6.
[55] *Wiebe*, ecolex 2017, 783f.

## *4.3 EU-Rechtsvorschriften und die Auswirkungen auf digitale Anwendungen / Serviceleistungen*

Die europäische Union hat seit der Initiierung der Maßnahmenpakete für den digitalen Binnenmarkt bereits einige Verordnungen und Richtlinien umgesetzt. Die im Zusammenhang mit digitalen Anwendungen/Serviceleistungen stehenden wichtigsten Regulierungen werden nachfolgend interpretiert.

Im Rahmen dieser Master Thesis werden die Auslegungen ausgewählter europarechtlicher Verordnungen und Richtlinien beurteilt, jedoch nicht die darauf basierenden nationalen Umsetzungen der Richtlinien in den Mitgliedstaaten eingegangen. Verordnungen sind ohnehin unmittelbar in den Mitgliedstaaten anwendbar und es bedarf keiner weiteren Umsetzung durch nationale Gesetzgebungsmaßnahmen.

## *4.4 Datenschutz-Grundverordnung*

Die hierzulande öffentlich verbreitete Verordnung im Bereich der Digitalisierung war die seit Mai 2018 unmittelbar in allen Mitgliedstaaten anwendbare neue Datenschutz-Grundverordnung (DSGVO). Diese Verordnung reguliert die „Verarbeitung" von personenbezogenen Daten, soweit sich diese innerhalb der Europäischen Union befinden.[56]

Gemäß Kapitel 1 Art. 4 Abs. 1 DSGVO sind personenbezogene Daten:
„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen […] insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind."[57]

Diese Regelung bezieht sich ausschließlich auf Daten, welche eindeutig einer bestimmten natürlichen Person zuzuordnen sind. Im Zuge der Datenverarbeitung durch digitale Anwendungen sind Daten mit unterschiedlichsten Merkmalen Gegenstand der Verarbeitung.

[56] Datenschutz-GrundVO 2016/679 ABI L 2016/119, 1.
[57] Datenschutz-GrundVO 2016/679 ABI L 2016/119, 32.

In diesem Zusammenhang betrachten wir in den folgenden Unterabschnitten beispielhaft den Anwendungsbereich von Industrie 4.0 Wartungs- und Instandhaltungsanwendungen.

### 4.4.1 Anwendungsbereich Condition Monitoring

Die Funktionsweise von Condition Monitoring wurde in den vorhergegangenen Kapiteln bereits beschrieben, weshalb sich dieses Kapitel auf die Anwendung der DSGVO beschränkt.

Grundsätzlich werden nicht-personenbezogene Daten, also Prozess- oder Maschinendaten, mittels Condition Monitoring-Anwendungen verarbeitet. Als ersten Schritt prüfen wir die Anwendbarkeit der DSGVO auf Condition Monitoring-Anwendungen, indem evaluiert wird, ob diese in den sachlichen und räumlichen Anwendungsbereich der Verordnung fällt.

Geht man davon aus, dass die erfassten Daten aufgrund einer fixen Position eines Sensors oder Aktors, den Standortdaten sowie Datum- und Zeitstempels als besonderes Merkmal, eindeutig identifiziert werden können und möglicherweise aufgrund von verfügbaren und abgestimmten Schichtplänen einer natürlichen Person eindeutig zugeordnet werden können (personenbezogene Daten), so müssten die Grundsätze der DSGVO berücksichtigt werden. Weiters ist zu hinterfragen, ob der Zutritt zur Anlage oder die Benützung der Industrie 4.0-Anwendung unter Angabe eines eindeutig einem Mitarbeiter zugeordneten Zugangscode passiert ist. Im Erwägungsgrund Nr. 26 DSGVO wird noch ergänzt, dass pseudonymisierte personenbezogene Daten unter bestimmten Bedingungen auch berücksichtigt und identifiziert werden müssen. Legt man diesen Sachverhalt weit aus, so kann dies durchaus einer „Psyeudonymisierung“ von Daten unterliegen.

Wenn man basierend auf dem angenommenen Sachverhalt davon ausgehen kann, dass es sich um personenbezogene bzw. eindeutig identifizierbare Daten handelt und diese durch die Condition Monitoring-Anwendung verarbeitet und gespeichert werden, so fällt es in den sachlichen Anwendungsbereich nach Art. 2 Abs. 1 DSGVO.

In den räumlichen Anwendungsbereich nach Art. 3 DSGVO fällt es, wenn wir davon ausgehen, dass die Tätigkeiten des Unternehmens innerhalb der Europäischen Union stattfinden.

Abgesehen von einer möglichen Anwendbarkeit der DSGVO in Spezialfällen sind bei branchenüblichen Condition Monitoring-Anwendungen keine bzw. nur sehr selten personenbezogene Daten im Spiel. Sollte der Fall dennoch eintreten, dass personenbezogene Daten verarbeitet werden, dann bleibt die Möglichkeit der Pseudonymisierung.

Bezugnehmend auf Art. 24 DSGVO „Verantwortung des durch die Verarbeitung Verantwortlichen" und Art. 25 DSGVO „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen" („privacy by design") ist bei der Entwicklung von Industrie 4.0-Anwendungen bereits im Vorfeld sicherzustellen, dass jegliche geeigneten technischen und organisatorischen Maßnahmen berücksichtigt werden, sowie datenschutzfreundliche Voreinstellungen beim Design von IIoT-Systemen (im Speziellen Software) vorgenommen werden, um eine unrechtmäßige Verarbeitung von personenbezogenen Daten auszuschließen.[58] Die Ausführung nach State-of-the-Art Design-Regeln (internationale Normen und Standards, datenschutzrechtliche Zertifizierungen) von IIoT-Anwendungen soll die Datensicherheit erhöhen und das Risiko von Datenverlusten eindämmen. Kommt es dennoch zu einer Datenschutzverletzung bzw. einem Datenverlust, so hat der Auftragsverarbeiter die Pflicht die betroffene Person unverzüglich zu benachrichtigen und auch nachzuweisen, dass die getroffenen Sicherheitsvorkehrungsmaßnahmen ausreichend umgesetzt worden sind.[59]

Bevor es überhaupt zu einer Datenschutzverletzung kommen kann, stellt sich die Frage, wie zwischen Prozess- oder Sensordaten und personenbezogenen Daten unterschieden wird? Die Priorität in der Verarbeitung von Daten haben für produzierende Unternehmen die nicht-personenbezogenen Daten. *Ensthaler* beschreibt als Handlungsempfehlung ein mögliches Szenario für Industrie 4.0-Anwendungen, welches einen Übermittlungsstandard definiert, der die Möglichkeit bietet Daten nach unterschiedlichen Informationen und Merkmalen zu kategorisieren. Für die einzelnen Daten-Kategorien kann dann individuell ein geeignetes Schutzniveau festgelegt und angewandt werden (beispielsweise können so sensible personenbezogene Daten und Prozess- oder Sensordaten gefiltert werden).[60]

[58] Datenschutz-GrundVO 2016/679 ABI L 2016/119, 48; 15.
[59] Datenschutz-GrundVO 2016/679 ABI L 2016/119, 52.
[60] *Ensthaler*, NJW 2016, 1.

Um sich als Unternehmen abzusichern und um Sanktionen aufgrund von unrechtmäßig verarbeiteten personenbezogenen Daten vorzubeugen, bestehen gemäß Art. 6 DSGVO u.a. folgende Möglichkeiten einer rechtmäßigen Verarbeitung:

> „a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
> b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen."[61]

Diese Ausnahmeregelungen der Einwilligung und Verarbeitung im Rahmen eines Vertrages (Zweckbindung) geben nicht nur dem Datenverarbeiter Rechtssicherheit, sondern verleihen der betroffenen Person das Recht und die Freiheit, die Verarbeitung von personenbezogenen Daten zu untersagen. Der Auftragsverarbeiter ist auf der Grundlage eines Vertrages gemäß Art. 28 DSGVO dazu berechtigt, die personenbezogenen Daten entsprechend der getroffenen vertraglichen Vereinbarung mit der betroffenen Person zu verarbeiten.[62] Die betroffenen Personen können sich das Recht vorbehalten, jederzeit Einsicht in die vom Auftragsverarbeiter verarbeiteten personenbezogenen Daten zu erhalten und diese in einem gängigen lesbaren Format direkt bereitgestellt zu bekommen.[63] Die DSGVO geht hier noch einen Schritt weiter und räumt der betroffenen Person das Recht ein, die schriftliche Einwilligungs-Erklärung jederzeit zu widerrufen (Art. 7 Abs. 3 DSGVO). Erfolgt die Verarbeitung als essentieller Bestandteil der vertraglich vereinbarten Leistung, so ist zu prüfen, inwieweit bei einem Widerruf der Einwilligung, die Erfüllung des Vertrags noch möglich ist.

Das Widerspruchsrecht gemäß Art. 21 DSGVO enthält in Abs. 6 eine Ausnahmeregelung, welche möglicherweise für Industrie 4.0-Anwendungen relevant sein kann. Erfolgt die Verarbeitung von Daten im Rahmen eines wissenschaftlichen F&E-Projekts und sind diese Informationen für die Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich[64], so kann die betroffene Person von seinem Widerspruchsrecht Gebrauch machen, jedoch nicht ohne Rechtfertigung durch einen besonderen Grund.

[61] Datenschutz-GrundVO 2016/679 ABI L 2016/119, 36.
[62] Datenschutz-GrundVO 2016/679 ABI L 2016/119, 49.
[63] Datenschutz-GrundVO 2016/679 ABI L 2016/119, 13.
[64] Datenschutz-GrundVO 2016/679 ABI L 2016/119, 45.

Nachdem die im Zusammenhang mit Condition Monitoring stehenden wichtigsten Regulierungen der DSGVO betrachtet wurden und für die Anwendungen wie Predictive Maintenance und Remote-Support weitgehend die gleichen Voraussetzungen bestehen, wird eine individuelle Auslegung der DSGVO in Bezug auf die zuvor genannten IIoT-Anwendungen im Rahmen dieses Kapitels nicht mehr durchgeführt, da idente Untersuchungsergebnisse erwarten werden können.

### 4.4.2 Anwendungsbereich Cloud-Computing

Die fortschreitende Digitalisierung ist mitverantwortlich dafür, dass wir uns in Europa auf dem Weg von einer Industrie- zu einer Dienstleistungsgesellschaft[65] befinden. Diese Entwicklung spiegelt sich auch bei IIoT-Anwendungen in der industriellen Produktion wider. Industrie 4.0-Anwendungen, wie Condition Monitoring, erfassen Daten von Geräten in der Produktion des Kunden, welche dann über ein Netzwerk verbreitet und in vielen Fällen außerhalb der Produktion in einer sogenannten Cloud gespeichert werden.

Der European Data Protection Board EDPB (ersetzt die Artikel-29-Datenschutzgruppe) hat sich mit der Nutzung von Cloud-Computing Diensten auseinandergesetzt und zahlreiche Stellungnahmen und Leitlinien veröffentlicht.[66]

Cloud-Computing ist definiert als IT-Infrastruktur (Datenspeicher, Rechenleistung) bzw. IT-Dienstleitung (IIoT-Anwendung, Software), die über das Internet an Endnutzer zur Verfügung gestellt wird.[67] Cloud-Computing in Verbindung mit IIoT-Anwendungen kann man sich in drei Ebenen vorstellen, nämlich der Geräte-, der Kommunikations- und der Speicherplatzebene (Cloud).

Es ist festzustellen, dass es mittlerweile eine große Auswahl an verschiedensten Cloud-Dienstleistern gibt, welche unterschiedlichste Cloud-Arten und Cloud-Dienstleistungen anbieten. Das *Fraunhofer-Institut* hat die verschiedenen Betriebsmodelle und Dienstleistungen in ihrer Studie im Detail erklärt und zusammengefasst. Die Cloud-Betriebsmodelle umfassen die "Public Cloud, Private Cloud, Community Cloud sowie die Hybrid Cloud und die

[65] *Ecker/Weyerstraß*: Kreative Zerstörung 4.0: Industrie 4.0 als Chance für eine stärkere Industrie, als Schlüssel für mehr Wettbewerbsfähigkeit, Wirtschaftspolitische Blätter (2016) 321ff
[66] *European Data Protection Board*, https://ec.europa.eu/newsroom/article29/news-overview.cfm
[67] *Raffling/Schock (Hrsg)*, Digitale Wirtschaft und Industrie 4.0 (2018) 47.

Dienstleistungen, wie Infrastructure as a Service (IaaS), Platform as a Service (PaaS) und Software as a Service (SaaS)".[68]

Im Rahmen dieser Master Thesis wird nicht näher auf die einzelnen Details dieser Modelle und Dienstleistungen eingegangen, sondern nur die Cloud als solches in die Auslegungen miteinbezogen.

Ergänzend zu den Cloud-Arten und Services sind rechtlich vor allem die Akteure „Cloud-Anbieter, Cloud-Anwender, Cloud-Endnutzer und Cloud-Kunde" von Interesse. Der Cloud-Anbieter ist charakterisiert durch eine natürliche- oder juristische Person, durch den Eigentümer oder Betreiber der Cloud, oder dem Dienstleister. Der Cloud-Anwender ist gekennzeichnet durch den Auftragsverarbeiter, welcher verantwortlich ist für die Verarbeitung von Daten, oder dem Dienstleister/Hersteller des IIoT-Systems. Der Cloud-Endnutzer ist verantwortlich für die Festlegung welche Daten vertraglich verarbeitet werden dürfen.[69]

Abgesehen von den genannten Akteuren kann es in Folge von Industrie 4.0-Anwendungen zu variierenden Vertragspartnern für die unterschiedlichen Cloud-Dienste kommen. Die wahrscheinlichste Variante ist der Vertrag zwischen dem Auftragsverarbeiter (meist Cloud-Anwender) und dem Cloud-Anbieter. Eine weitere Möglichkeit besteht darin, dass der Cloud-Endnutzer direkt einen Vertrag mit dem Cloud-Anbieter abschließt. Rechtliche Grundlage für die Verarbeitung von Daten in einer Cloud ist demnach ein Cloud-Nutzungsvertrag. Unabhängig von den beteiligten Vertragsparteien ist zu beachten, dass dieser Cloud-Nutzungsvertrag eine detaillierte Leistungsbeschreibung für die angebotene Dienstleistung und speziell für die Verarbeitung von personenbezogenen Daten beinhaltet. Damit gewährleistet wird, dass die Cloud State-of-the-Art Datenschutz-Sicherheitsstandards und Transparenz-Anforderung erfüllt, ist es ratsam nur entsprechend durch eine akkreditierte Stelle zertifizierte[70] Cloud-Anbieter auszuwählen.

Durch die Nutzung eines Cloud-Dienstes sind die personenbezogenen Daten nun nicht mehr lokal auf einem Rechner gespeichert, sondern in der Cloud des Cloud-Anbieters. Wichtig zu

[68] *Fraunhofer Institut für Offene Kommunikationssysteme*, ISPRAT-Studie, Cloud-Computing für die öffentliche Verwaltung (2010) 20ff.
[69] *Raffling/Schock (Hrsg)*, Digitale Wirtschaft und Industrie 4.0 (2018) 47f.
[70] Datenschutz-GrundVO 2016/679 ABI L 2016/119, 58.

beachten ist, dass der Cloud-Nutzer (Verantwortlicher) für die Einhaltung des geltenden Datenschutzrechts verantwortlich bleibt und nicht der Cloud-Anbieter (Auftragsverarbeiter). Verarbeitet bzw. bearbeitet der Cloud-Diensteanbieter personenbezogene Daten, dann fällt auch dieser in den Anwendungsbereich der DSGVO.[71]

Am bereits in Kapitel 4.2 auf Seite 25/26 skizzierten Beispiel wollen wir nun ein mögliches Szenario analysieren. In unserem Beispiel wird die IIoT-Anwendung von einem Automobilzulieferer genutzt, welcher der rechtlich Verantwortliche für die Daten ist und festlegt, welche Partei welche Art von Daten rechtmäßig verarbeiten darf. Der Industrieofen-Hersteller ist der Auftragsverarbeiter iSd DSGVO und verarbeitet für die Erbringung seiner vertraglichen Dienstleistung die personenbezogenen und nicht-personenbezogenen Daten. Für die Datenspeicherung wird eine Cloud ausgewählt. Somit besteht ein Vertrag zwischen dem Automobilzulieferer und dem Industrieofen-Hersteller, sowie dem Industrieofen-Hersteller und dem Cloud-Dienstleister. Wird durch den Cloud-Dienstleister auch eine Verarbeitung der personenbezogenen Daten durchgeführt, so ist das nur mit vorheriger schriftlicher Genehmigung des Verantwortlichen (Automobilzulieferers) gemäß Art. 28 Abs. 2 DSGVO möglich, da dieser dann zu einem Unterauftragnehmer wird. Es ist zu beachten, dass dem Unterauftragnehmer die gleichen vertraglichen Rechte auferlegt werden wie dem Auftragsverarbeiter selbst durch den Verantwortlichen.[72] Der Cloud-Dienstleister hat in diesem Fall dafür Sorge zu tragen, dass geeignete technische und organisatorische Maßnahmen eingesetzt werden, um den Datenschutzrechten der betroffenen Person nachzukommen. Die Auftragsverarbeiter sind an die Weisungen des Verantwortlichen gebunden.[73]

In der bisherigen Betrachtung bis dato unberücksichtigt gelassen wurden Serverstandorte der Cloud-Dienstleister. Diese sind durchaus von rechtlicher Relevanz und maßgebend für die Angemessenheit des Schutzes. Datenschutzrechtlich relevant sind in diesem Zusammenhang vor allem der Transfer von personenbezogenen Daten auf Clouds mittels Server in Drittländern. Die DSGVO definiert hierzu Bedingungen für den Verantwortlichen und den Auftragsverarbeiter, als Grundlage für einen rechtmäßigen und uneingeschränkten

[71] *Eckhardt/Höllwarth/Laux/Thiele*, Cloud & Datenschutz. Der Cloud Privacy Check (CPC) (2017) 6f.
[72] Datenschutz-GrundVO 2016/679 ABI L 2016/119, 49.
[73] Datenschutz-GrundVO 2016/679 ABI L 2016/119, 49.

Datenverkehr in ein Drittland. Dabei wird festgelegt, dass zumindest das durch die DSGVO gewährleistete Schutzniveau auch im Drittland sicherzustellen ist.[74]

## *4.5 Freier Verkehr nicht-personenbezogener Daten*

Nachdem die DSGVO zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten seit 25. Mai 2018 unmittelbar in den Mitgliedstaaten der europäischen Union anwendbar ist, hat die Europäische Kommission im nächsten Schritt für die Bereitstellung eines weitreichenden Rechtsrahmens für den digitalen Binnenmarkt, auch eine Verordnung erlassen, welche den freien Verkehr von nicht-personenbezogenen Daten („free flow of non-personal data“) reguliert, die von der DSGVO nicht erfasst sind. Die Verordnung 2018/1807[75] ist am 18. Dezember 2018 in Kraft getreten.

Diese sachliche Regelung soll im Hinblick auf die zunehmende Digitalisierung, der globalen Vernetzung, der intelligenten Fabriken und der florierenden Datenwirtschaft einen maßgeblichen rechtlichen Rahmen für die Realisierung eines freien, sicheren und zuverlässigen Datenverkehrs[76] innerhalb des EU-Binnenmarktes schaffen.

In diesem Abschnitt werden die Regulierungen dieser Verordnung in Zusammenhang mit Industrie 4.0-Anwendungen genauer betrachtet.

Nicht-personenbezogene Daten im Maschinen- und Anlagenbau umfassen vor allem maschinengenerierte Daten (Maschinen-, Prozess- oder Sensordaten). Ob es sich um personenbezogene oder nicht-personenbezogene Daten handelt kann dahingehend festgestellt werden, indem der Bezug der in Frage stehenden Daten zu einer natürlichen Person geprüft wird. Ergibt die Prüfung einen Bezug zu einer natürlichen Person, dann ist die DSGVO anwendbar, solange die Daten nicht vollständig anonymisiert wurden (im Falle einer Pseudonymisierung ist die DSGVO weiter anwendbar).[77] Diese Zustandsdaten von Anlagen sind für Industrie 4.0-Anwendungen wesentlich und stellen mittlerweile einen enormen wirtschaftlichen Wert für die Unternehmen dar. Die Menge an verarbeiteten Daten in der

[74] Datenschutz-GrundVO 2016/679 ABI L 2016/119, 60.
[75] FreierDatenverkehrVO 2018/1807 ABI L 2018/303, 59.
[76] *Europäische Kommission*, COM(2017) 9 final, 5f.
[77] *Europäische Kommission*, COM(2017) 9 final, 10.

industriellen Fertigung ist bei maschinengenerierten nicht-personenbezogenen Daten bedeutend höher als bei personenbezogenen Daten. Diese Datenflut an anonymen Daten gilt es zu regulieren und in geordnete rechtliche Bahnen zu lenken. Wie in Kapitel 4.2 bereits näher ausgeführt, entstehen durch den intensiven Datenaustausch entlang der horizontalen bzw. vertikalen Wertschöpfungskette auch potentielle kartell- und wettbewerbsrechtliche Herausforderungen.

Die VO 2018/1807 hebt nochmals hervor, dass die Grundfreiheiten der Niederlassungsfreiheit und der Dienstleistungsfreiheit auch für die Verarbeitung von Daten gelten, jedoch aufgrund nationaler Gesetzgebungen der Mitgliedstaaten häufig rechtlich eingeschränkt sind.[78]

Die Richtlinie regelt weiters die Anwendbarkeit auf unterschiedlichste IT-Systeme (hierunter fallen auch Industrie 4.0-Anwendungen sowie Cloud-Computing), welche Daten speichern oder verarbeiten.[79]

Der Art. 1 VO 2018/1807 regelt die „Vorschriften über Datenlokalisierungsauflagen, die Verfügbarkeit von Daten für zuständige Behörden und die Übertragung von Daten für berufliche Nutzer“.[80]

Zum Gegenstand dieser Verordnung ist anzumerken, dass Datenlokalisierungsauflagen („eine Verpflichtung, ein Verbot, eine Bedingung, eine Beschränkung in den nationalen Rechts- und Verwaltungsvorschriften“[81]) grundsätzlich unzulässig[82] sind und nur unter bestimmten Bedingungen in Ausnahmen gerechtfertigt sein können.

Wesentlich für den Anwendungsbereich dieser VO 2018/1807 für Industrie 4.0-Anwendungen ist die Tatsache, dass die DSGVO weiter anzuwenden ist, wenn sich ein Datensatz aus untrennbar miteinander verbundenen personenbezogenen und nicht-personenbezogenen Daten zusammensetzt.[83]

[78] FreierDatenverkehrVO 2018/1807 ABI L 2018/303, 59.
[79] FreierDatenverkehrVO 2018/1807 ABI L 2018/303, 61.
[80] FreierDatenverkehrVO 2018/1807 ABI L 2018/303, 65.
[81] FreierDatenverkehrVO 2018/1807 ABI L 2018/303, 65.
[82] FreierDatenverkehrVO 2018/1807 ABI L 2018/303, 66.
[83] FreierDatenverkehrVO 2018/1807 ABI L 2018/303, 65.

Bei der Übertragung von nicht-personenbezogenen Daten setzt die Europäische Kommission ganz auf die Selbstregulierung durch Entwicklung von Verhaltensregeln. Die Verordnung gibt diesbezüglich nur einen Leitfaden mit Mindestinhalten vor, die sich an den Verhaltensregeln gemäß Art. 40 DSGVO orientieren und fordert eine Entwicklung von Verhaltensregeln durch die Diensteanbieter bis 29. Mai 2020.[84] Die Grundsätze enthalten u.a. Anforderungen wie einen „Einfachen Anbieterwechsel" (Abs. 1 lit a), die „Nutzung eines gängigen Übertragungsformats" (Abs. 1 lit a), dem „Abschluss eines Datenverarbeitungsvertrags für berufliche Nutzer mit transparenten Informationen über Prozesse und technische Anforderungen" (Abs. 1 lit b), einer „Zertifizierungsmöglichkeit" (Abs. 1 lit c) oder „Kommunikationsplänen" (Abs. 1 lit d).[85]

Zusammenfassend ist festzuhalten, dass durch diese „free flow of non-personal data"-Verordnung ein weiterer Rechtsrahmen für die Verwirklichung des digitalen Binnenmarktes hinzugekommen ist, welche sich stark an der DSGVO orientiert. In Bezug auf Industrie 4.0-Anwendungen und die Verarbeitung von nicht-personenbezogenen Daten ist diese Verordnung u.a. bei Themen wie dem Zugang zu maschinengenerierten Daten, dem Dateneigentum, der Technikgestaltung oder der Datenübertragung sehr vage und enthält keine wesentlichen Einschränkungen für den freien Datenverkehr von nicht-personenbezogenen Daten.[86] Die Europäische Kommission plant in diesem Zusammenhang keine weiteren detaillierten technischen Vorschriften, sondern forciert die Selbstregulierung und verweist auf die Entwicklung der Verhaltensregeln bis Anfang des Jahres 2020.[87]

## *4.6 Vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen*

Diese relativ neue Richtlinie 2019/770 (seit 11.6.2019 in Kraft), welche in den einzelnen Mitgliedstaaten entsprechend in der nationalen Gesetzgebung umgesetzt werden muss, wurde mit dem vorrangigen Ziel der Angleichung der Verbrauchervorschriften und der Etablierung eines harmonisierten und auf den digitalen Anforderungen angepasstes Gewährleistungsrecht innerhalb des digitalen Binnenmarktes geschaffen. Gleichzeitig mit der RL 2019/770 ist auch

[84] FreierDatenverkehrVO 2018/1807 ABI L 2018/303, 67.
[85] FreierDatenverkehrVO 2018/1807 ABI L 2018/303, 67.
[86] *Staudegger*, jusIT 2019, 8f.
[87] FreierDatenverkehrVO 2018/1807 ABI L 2018/303, 60.

die Warenkauf-RL 2019/771, die vertragliche Aspekte des Warenkaufs berücksichtigt, in Kraft getreten.[88] Die RL 2019/771 wird folglich im Rahmen dieser Master Thesis nicht weiter betrachtet.

### 4.6.1 Anwendungsbereich der Richtlinie

Die RL 2019/770 ist anwendbar auf zwischen Unternehmen und Verbrauchern abgeschlossenen Verträgen mit digitalen Inhalten und digitalen Dienstleistungen und ist auf diesen Anwendungsbereich auch beschränkt.[89] Diese Regulierung ist somit nicht für den B2B-Bereich anwendbar, obwohl auch in diesem Bereich vertragsrechtlich Nachholbedarf besteht. Die Rechte von Unternehmen (im Gegensatz zu den Pflichten) bleiben weitgehend unberücksichtigt. Die vertragliche Ausgestaltung im B2B-Bereich findet überwiegend durch Kauf- oder Werksverträge statt.[90]

Da einige Regelungsaspekte der Richtlinie durchaus Anhaltspunkte für die B2B Vertragsgestaltung darstellen, wird die Prüfung im Rahmen dieser Master Thesis weiter fortgeführt.

Digitale Inhalte werden in der Richtlinie als „in digitaler Form erstellte und bereitgestellte Daten“[91] bezeichnet. In dieser Definition fällt auf, dass die Daten dieser digitalen Inhalte nur erstellt (z.B. erfasst durch Sensoren) und bereitgestellt (z.B. an die Industrie 4.0-Anwendung) werden, aber nicht verarbeitet. Industrie 4.0-Anwendungen, die gewöhnlich Daten verarbeiten, würden somit nicht als „Digitale Inhalte“ zu bezeichnen sein.

Digitale Dienstleistungen werden in der Richtline folgendermaßen definiert:
„die dem Verbraucher die Erstellung, Verarbeitung oder Speicherung von Daten in digitaler Form oder den Zugang zu solchen Daten ermöglichen oder Dienstleistungen, die die gemeinsame Nutzung der vom Verbraucher oder von anderen Nutzern der entsprechenden

[88] Richtlinie (EU) 2019/771 des europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte des Warenkaufs, zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie 2009/22/EG sowie zur Aufhebung der Richtlinie 1999/44/EG ABI L 2019/136, 28.
[89] DigitaleInhalteRL 2019/770 ABI L 2019/136, 17.
[90] *Metzger*, DJZ 2019, 578f.
[91] DigitaleInhalteRL 2019/770 ABI L 2019/136, 17.

Dienstleistung in digitaler Form hochgeladenen oder erstellten Daten oder sonstige Interaktionen mit diesen Daten ermöglichen."[92]

Industrie 4.0-Anwendungen verarbeiten Daten in digitaler Form und werten diese Daten im Hinblick auf proaktive Instandhaltungs- und Wartungsmaßnahmen auch aus („sonstige Interaktionen") und sind deshalb als digitale Dienstleistungen im Sinne der RL 2019/770 einzustufen. Sensoren oder Aktoren, also Komponenten, welche die maschinengenerierten Daten schaffen, sind im Sinne der RL 2019/770 „Waren mit digitalen Elementen".[93]

### 4.6.2 Vertragsbeendigungspflichten

Die Richtlinie behandelt zahlreiche Regulierungen, welche im Einklang mit der Bereitstellung personenbezogener Daten stehen und verweist hier mitunter auf die rechtlichen Anforderungen der DSGVO. Hinsichtlich der Tatsache, dass für den Zweck von Industrie 4.0-Anwendungen vorrangig maschinengenerierte nicht-personenbezogene Daten bereitgestellt und verarbeitet werden, liegt der Fokus in der Interpretation der Richtlinie auf den nicht-personenbezogenen Daten. Auf die Behandlung personenbezogener Daten wird deshalb in der folgenden Bewertung nicht mehr explizit eingegangen.

Daten werden in den Vertragsbeendigungspflichten für Unternehmer (Art. 16 RL 2019/770) wie folgt behandelt:

- „Personenbezogene Daten sind im Sinne der Regulierungen der DSGVO zu behandeln (Art. 16 Abs. 2)
- Bei nicht-personenbezogenen vom Verbraucher bereitgestellten Daten dürfen diese vom Unternehmer nicht mehr verwendet werden, es sei denn
    - diese Daten haben abgesehen vom verwendeten Zweck keinen weiteren Nutzen (Art. 16 Abs. 3 lit a)
    - sind auf die Nutzung der bereitgestellten Dienste durch den Verbraucher beschränkt (Art. 16 Abs. 3 lit b)
    - wurden vom Unternehmer mit anderen Daten verarbeitet und sind nur mit unverhältnismäßigem Aufwand wieder zu trennen (Art. 16 Abs. 3 lit c)

[92] DigitaleInhalteRL 2019/770 ABI L 2019/136, 17.
[93] DigitaleInhalteRL 2019/770 ABI L 2019/136, 17.

- es handelt sich um Gemeinschaftsdaten mehrerer Verbraucher und andere Verbraucher können diese noch nutzen (Art. 16 Abs. 3 lit d)“[94]

Unter Berücksichtigung der Ausnahmen (Art. 16 Abs. 3 lit a,b,c RL 2019/770) ist der Unternehmer im Fall einer Vertragsbeendigung dazu verpflichtet, die nicht-personenbezogenen Daten, die im Rahmen der digitalen Dienstleistung verwendet wurden, dem Verbraucher auf dessen Anfrage kostenfrei in einem gängigen Format bereitzustellen.

Einen wesentlichen Teil der RL 2019/770 bildet die Harmonisierung der Gewährleistungsbedingungen innerhalb des EU-Binnenmarktes, welche mit dieser Richtlinie nun auch auf digitale Inhalte und Dienstleistungen ausgeweitet wurden.

Sind die subjektiven und objektiven Anforderungen an die bereitgestellten digitalen Inhalte oder digitalen Dienstleistungen nicht wie vereinbart erfüllt, so ist das Vorliegen einer Vertragswidrigkeit zu prüfen.[95]

### 4.6.3 Haftungsbedingungen und Abhilfemaßnahmen

Die RL 2019/770 legt die Haftungsbedingungen in Art. 11 fest. Diese umfassen den Anspruch auf einen Gewährleistungszeitraum von mindestens zwei Jahren ab der Bereitstellung, unabhängig davon ob eine einmalige oder mehrmalige Bereitstellung der vereinbarten digitalen Inhalte oder Dienstleistung vorliegt. Besteht in einem nationalen Recht nur eine Verjährungsfrist, so muss auch diese zumindest zwei Jahre betragen und die Möglichkeit bestehen in dieser Zeit Abhilfemaßnahmen in Anspruch zu nehmen.[96] Zunächst gilt die Beweislast durch den Unternehmer innerhalb des ersten Jahres ab der Bereitstellung. Die Ursachenfeststellung hat gemeinsam durch den Unternehmer und dem Verbraucher in einem verhältnismäßigen Ausmaß stattzufinden.[97]

[94] DigitaleInhalteRL 2019/770 ABI L 2019/136, 24.
[95] DigitaleInhalteRL 2019/770 ABI L 2019/136, 20f.
[96] DigitaleInhalteRL 2019/770 ABI L 2019/136, 21f.
[97] DigitaleInhalteRL 2019/770 ABI L 2019/136, 22.

Bei Zuwiderhandeln besteht der Anspruch auf Abhilfemaßnahmen (Art. 14) der ersten Stufe: Wiederherstellung des Vertragszustandes (sofern verhältnismäßig) und der zweiten Stufe: Preisminderung oder Vertragsbeendigung.[98]

Diese Richtlinie bietet vor allem Verbrauchern zusätzliche Rechte bei der Nutzung von digitalen Inhalten und digitalen Dienstleistungen, jedoch sind die Auswirkungen auf den EU-Binnenmarkt für Unternehmen und Verbraucher erst ab dem 1. Januar 2022 zu spüren, wenn diese Richtlinie in allen Mitgliedstaaten umgesetzt ist.[99]

## *4.7 Urheberrecht und Schutzrechte im digitalen Binnenmarkt*

In Zusammenhang mit Datenschutzrechten sind auch mögliche Interessenskonflikte bzgl. der Verarbeitung von vertraulichen Informationen, wie Betriebs- oder Geschäftsgeheimnissen bzw. Immaterialgüterrechten zu bewerten.

Hierzu hat die Europäische Union die RL 2019/790 über das Urheberrecht und verwandte Schutzrecht im digitalen Binnenmarkt im Jahr 2019 veröffentlicht. Eine Umsetzung dieser EU-Richtlinie in den nationalen Jurisdiktionen ist bis zum 7. Juni 2021 durchzuführen.[100]

### 4.7.1 Anwendungsbereich der Richtlinie

Industrie 4.0-Anwendungen, wie z.B. Condition Monitoring oder Predictive Maintenance, setzen Data Mining-Methoden („automatisierte Analyse von Daten in digitaler Form“[101]) zur Analyse und Auswertung von Daten, sowie Ableitung von Maßnahmen für die industrielle Produktion ein. Abgesehen von Regulierungen hinsichtlich Data Mining in der wissenschaftlichen Forschung, befasst sich diese Richtlinie mit urheberrechtlichen Fragen zu nicht-personenbezogenen, maschinengenerierten Daten. Inwieweit die im Rahmen von Industrie 4.0-Anwendungen verarbeiteten Daten urheberrechtlich einen Schutzgegenstand darstellen, ist nicht Umfang dieser Richtlinie.

[98] DigitaleInhalteRL 2019/770 ABI L 2019/136, 23.
[99] *Kern/Maier*, Zak 2019, 210.
[100] UrheberrechtsRL 2019/790 ABI L 2019/130, 92.
[101] UrheberrechtsRL 2019/790 ABI L 2019/130, 112.

Die mögliche Antwort auf die Frage, ob maschinengenerierte Daten urheberrechtlich geschützt werden können, kann womöglich die Richtlinie 96/9/EG über den rechtlichen Schutz von Datenbanken geben. Einführend wird dazu eine etwas ältere EuGH-Entscheidung aus dem Jahre 2012 analysiert und auf dieser Grundlage ein Vergleich mit Industrie 4.0-Anwendungen angestellt.

### 4.7.2 Rechtssache Football Dataco Ltd.

In der Rechtssache C-604/10 (zwischen u.a. Football Dataco Ltd u. a. und Yahoo! UK Ltd), bei der es um einen möglichen urheberrechtlichen Schutz eines Spielplans für Fußballspiele geht, welche in einer Datenbank gespeichert sind, entscheidet der Europäische Gerichtshof, dass diese Inhalte (Spielplan für Fußballspiele) nicht urheberrechtlich geschützt werden können. In seinem Urteil stellt der EuGH darauf ab, dass weder ein urheberrechtlicher Schutz für die Datenbank selbst gewährt werden kann, noch für den Inhalt der Datenbank.[102]

Das Kriterium der „Originalität im Sinne der geistigen Schöpfung“[103] als Voraussetzung für den urheberrechtlichen Schutz einer Datenbank gemäß der Richtlinie 96/9/EG ist demnach nicht erfüllt („die Beurteilung erstreckt sich nicht auf die Daten selbst“[104]). Darüber hinaus erfüllt auch die Erstellung der Spielpläne nicht das Kriterium einer ausreichenden geistigen Leistung.
Die Voraussetzung für den Schutz von Daten ist die Existenz einer Sammlung von Daten (oder einer Zusammenstellung)[105]. Außerdem kommt es darauf an, dass diese Sammlung durch eine wesentliche Investition[106] geschaffen worden ist.

Gemäß der Auslegung des Europäischen Gerichtshofs in der Rechtssache C-604/10 und im Sinne der Richtlinie 96/9/EG sind bei digitalen IIoT-Anwendungen bzw. Serviceleistungen Prüfungsschritte durchzuführen, um festzustellen, ob ein Anspruch auf urheberrechtlichen Schutz besteht. Zunächst muss geprüft werden, ob die gesammelten nicht-personenbezogenen Daten als eine Sammlung oder Zusammenstellung von Daten zu betrachten sind. Ein solcher Anspruch setzt weiter voraus, dass die Sammlung durch eine wesentliche Investition

[102] EuGH 1.3.2012, C-604/10 Football Dataco Ltd
[103] Richtlinie 96/9/EG des Europäischen Parlaments und des Rates vom 11. März 1996 über den rechtlichen Schutz von Datenbanken ABI L 1996/77, 21.
[104] *Gerichtshof der Europäischen Union*, Pressemitteilung Nr. 16/12, 2012
[105] DatenbankenschutzRL 96/9/EG ABI L 1996/77, 24; 21.
[106] DatenbankenschutzRL 96/9/EG ABI L 1996/77, 25f.

geschaffen worden und das Kriterium der Originalität im Sinne einer geistigen Schöpfung für diese Daten erfüllt ist.

*Ensthaler* legt die Richtlinie bzw. das Gerichtsurteil so aus, dass eine gewisse Systematik der Sammlung von Daten, im Sinne einer Ordnerstruktur, schon auf das Vorhandensein einer Sammlung hindeutet. Das Datenbankschutzrecht per se schützt jedoch nicht den Inhalt (Daten), sondern nur die Datenbank selbst. Weiters ist auch das Investitionserfordernis nicht auf die Erfassung der Daten zu beziehen, sondern auf die Herstellung der Datenbank. Das Datenbankschutzrecht gibt daher keine Auskunft über die Schutzwürdigkeit von einzelnen nicht-personenbezogenen Daten.[107]

### 4.7.3 Sichtweise der Europäischen Kommission

Die Europäische Kommission stellt in ihrer Mitteilung „COM(2017) 9 final" zum „Aufbau einer europäischen Datenwirtschaft" fest, dass maschinengenerierte Rohdaten, aufgrund des Fehlens einer Originalität bzw. einer geistigen Leistung, nicht als geistiges Eigentum geschützt werden können.[108] Vorbehaltlich der nationalen Umsetzung der Richtlinie in den Mitgliedstaaten werden gemäß der Richtlinie (EU) 2016/943 vertrauliches Know-how und vertrauliche Geschäftsgeheimnisse vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung geschützt.[109] Dazu müssten also, abhängig von der nationalen Umsetzung der Richtlinie, Daten als geistiges Eigentum, Datenbank oder als Geschäftsgeheimnis im Sinne dieser Regelung gelten, um das Schutzbedürfnis zu erfüllen. Inwieweit diese Bedingungen von maschinengenerierten Daten erfüllt werden können, ist im Einzelfall zu prüfen.[110]

Im Sinne einer Umsetzung der Idee eines freien Datenverkehrs, kann alternativ die Gewährung eines Zugangs zu den Daten gegen Entgelt eine geeignete Möglichkeit darstellen. Diese Regelung müsste die Behandlung von vertraulichen Daten und die Interessen der Unternehmen in den Überlegungen berücksichtigen.

[107] *Ensthaler*, NJW 2016, 3.
[108] *Europäische Kommission*, COM(2017) 9 final, 11.
[109] Richtlinie (EU) 2016/943 des europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung ABI L 2016/157, 1.
[110] *Europäische Kommission*, COM(2017) 9 final, 11.

Fortführend ist eine Deklaration von maschinengenerierten Daten als Geschäftsgeheimnis schwierig, da die Voraussetzungen u.a. aufgrund der fehlenden Zuordnung zum Unternehmen („Inhaber des Geschäftsgeheimnisses“)[111] nicht gegeben sind und somit keine Schutzwirkung besteht.[112]

## *4.8 Vertragsrechtliche Handlungsempfehlungen*

Die, in den vorherigen Teilabschnitten betrachteten, europarechtlich auf digitale Anwendungen im Binnenmarkt anzuwendende Richtlinien und Verordnungen sind überwiegend weit ausgelegt und lassen einen eingeschränkten Interpretationsspielraum offen. Nichtsdestotrotz geben diese Rechtsgrundlagen auch für den Bereich digitaler Anwendungen und Dienstleistungen eine unmissverständliche Richtung, unter Berücksichtigung der Freiheiten von natürlichen Personen, vor.

Folgend werden zu den einzelnen Richtlinien und Verordnungen vertragliche Handlungsempfehlungen für den speziellen Anwendungsfall von Industrie 4.0-Anwendungen gegeben.

### 4.8.1 Datenschutz

Anwender von Industrie 4.0-Anwendungen sind üblicherweise nicht an der Verarbeitung von personenbezogenen und sensiblen Daten interessiert, da diese in den meisten Szenarien keinen Beitrag zur Funktionsweise dieser digitalen Systeme in industriellen Produktionsprozessen leisten. Vorrangig sind deshalb, in Bezug auf die DSGVO, die Beachtung der Anforderungen an die Datensicherheit und Kommunikation von Daten.

Sind in Ausnahmefällen dennoch personenbezogene Daten für die Zwecke der Industrie 4.0-Anwendung und zur Erreichung der Ziele zwingend notwendig und fallen somit in den Anwendungsbereich der DSGVO, dann ist soweit möglich eine Anonymisierung[113] oder Pseudonymisierung der Daten durchzuführen.[114]

[111] *Ensthaler*, NJW 2016, 4.
[112] Know-how-SchutzRL 2016/943 ABI L 2016/157, 1.
[113] Datenschutz-GrundVO 2016/679 ABI L 2016/119, 5.
[114] *Graf/Križanac*, ecolex 2017, 913.

Wird beispielsweise einem Automobilzulieferer in der produzierenden Industrie (=Kunde der IIoT-Anwendung) von dessen Kunde (möglicherweise Endverbraucher) ein fehlerhaftes Produkt gemeldet, so besteht auf Grundlage der gespeicherten und verarbeiteten Daten aus den digitalen Anwendungen die Möglichkeit zurückzuverfolgen, aus welcher Charge das fehlerhafte Teil kommt, wer die Anlage in dieser Schicht bedient und wer die Qualitätsprüfung/Qualitätssicherung durchgeführt hat. Die Chargeninformation wird vom IIoT-System verarbeitet, jedoch kommen die sensiblen personenbezogenen Schicht- bzw. Qualitätsprüfungsdaten üblicherweise vom Automobilzulieferer und werden nicht zwingend an das IIoT-System übertragen. Der Zweck der IIoT-Anwendung ist es prinzipiell nicht die in Frage stehenden personenbezogenen Daten zu verarbeiten und auszuwerten, sondern bezugnehmend auf das skizzierte Fallbeispiel aufgrund von Maschinen- und Prozessdaten festzustellen, welches Maschinenverhalten bzw. welcher Zustand ursächlich für das fehlerhafte Teil sein könnte. Ausgehend von diesem und ähnlichen Sachverhalten ist in Abstimmung mit dem Vertragspartner, eine gemeinsame Klassifizierung der Daten sowie die Festlegung der gewünschten Verarbeitung und der Schutzniveaus erforderlich.[115]

### 4.8.2 Definition von Vertragsbestandteilen

Erfordern digitale Anwendungen bzw. Serviceleistungen zur Leistungserfüllung die Verarbeitung personenbezogener Daten, so bedarf es im Vertrag einer unmissverständlichen Festlegung von Verantwortlichkeiten. Außerdem sind die Definition der Rechte und Pflichten der Vertragspartner in Bezug auf die Verarbeitung von personenbezogenen Daten wie z.B. Gegenstand und Dauer, Zweck, Art der Datenkategorien, Informationspflichten, Verarbeitung, Speicherung, Löschung, Verbreitung, Sicherheitsmaßnahmen und Vertraulichkeitsvereinbarungen, zu berücksichtigen. Damit die Verarbeitung der personenbezogenen Daten schlüssig nachvollziehbar und für alle Beteiligten transparent und richtig ist, wird die Einhaltung des Transparenzgebots gemäß Art. 5 Abs. 1 lit a DSGVO verlangt.

Ergänzend zu den zuvor angeführten Vertragspunkten sind für Cloud-Nutzungsverträge noch die Inhalte wie „Service Level Agreements (SLA), Information über Verträge mit Unterauftragnehmern, die Spezifikation technischer und organisatorischer Maßnahmen, EU-

[115] *Maurer/Pollirer*, Dako 2019, 50.

Standardvertragsklauseln (vor allem bei Datentransfers in Drittländern) und Geheimhaltungsvereinbarungen“[116] wesentlich zu berücksichtigen.

Findet die Verarbeitung von personenbezogenen Daten keine vertragliche Berücksichtigung, so kann die Einwilligung[117] mittels einer schriftlichen Willenserklärung, welche klar und unmissverständlich formuliert werden muss, durchgeführt werden.
Als Unternehmen (gemäß Art. 30 Abs. 5 DSGVO erst ab 250 Mitarbeitern) ist ein Verzeichnis mit allen Daten-Verarbeitungstätigkeiten verpflichtend zu führen.[118] Es ist nicht von Nachteil, wenn dieses Verzeichnis auch in kleineren Organisationen geführt wird, um einen Überblick über die datenverarbeitenden Vorgänge zu bekommen und ggfls. Untersuchungen bei nicht nachvollziehbaren Vorgängen einzuleiten.

Kann bereits im Vorfeld das Risiko einer möglichen Verletzung von Datenrechten nicht ausgeschlossen werden, so ist gemäß Art. 35 DSGVO eine Datenschutz Folgeabschätzung (Beschreibung der Verarbeitungsvorgänge, Bewertung von Zweck und Risiken, geplante Vorkehrungsmaßnahmen) durchzuführen.[119]

Die genaue Vorgehensweise, wie mit einem Widerruf bzw. einer Verletzung des Schutzes von personenbezogen Daten umgegangen wird, ist vorab festlegen, um im Falle einer Datenschutzverletzung unverzüglich reagieren zu können.

### 4.8.3 Design Anforderungen an IIoT-Anwendungen

Die relevanten und aktuellen Design-Rules („privacy by design“) sind bei der Erstellung von Industrie 4.0-Anwendungen zu berücksichtigen und sofern verfügbar, ist die Durchführung von Zertifizierungen für die Anwendungen anzustreben, um den geforderten Datensicherheitsanforderungen zu entsprechen, Transparenz zu schaffen und das Risiko einer möglichen Datenschutzverletzung damit zu minimieren. Datensicherheitskonzepte müssen am aktuellen Stand der Technik in allen Produktlebensphasen, von der Entwicklung bis zur Anwendung, berücksichtigt werden. Hierbei ist zwischen dem rechtlichen Datenschutz und der technischen Datensicherheit zu differenzieren, da diese auch unterschiedliche Schutzkonzepte

[116] *Raffling/Schock (Hrsg)*, Digitale Wirtschaft und Industrie 4.0 (2018) 51.
[117] Datenschutz-GrundVO 2016/679 ABI L 2016/119, 32.
[118] Datenschutz-GrundVO 2016/679 ABI L 2016/119, 50.
[119] Datenschutz-GrundVO 2016/679 ABI L 2016/119, 53.

verlangen. U.a. aufgrund von Haftungsfragen ist das Thema Sicherheit von IT-Systemen als äußerst kritisch einzustufen, weshalb alle erforderlichen Maßnahmen zum Schutz vor Angriffen auf die Daten getroffen werden müssen, um die Datensicherheit zu garantieren. Technische Schutzmaßnahmen wie die Sicherstellung einer zuverlässigen Kommunikation durch Verschlüsselungsalgorithmen, die Implementierung einer Zwei-Wege-Authentifizierung oder physischer Zugangs- und Kontrollkonzepte[120], sind für das sichere Funktionieren von IIoT-Systemen notwendig.
Die Agentur der Europäischen Union für Cybersicherheit ENISA hat dazu zahlreiche Publikationen und Leitlinien veröffentlicht. Hierbei wird sowohl auf die technische Umsetzung sicherheitsrelevanter Standards im IoT-Bereich (z.B. in der Publikation „Good Practices for Security of Internet of Things in the context of Smart Manufacturing"[121]) als auch auf grundsätzliche Handlungsempfehlungen für die Implementierung von Datensicherheitsmaßnahmen und Nutzung von Engineering-Methoden eingegangen (z.B. in der Publikation „Privacy and Data Protection by Design – from policy to engineering" [122]).

Im Falle von IIoT-Anwendungen und Dienstleistungen ist es zielführend in einem schriftlichen Vertrag Standard-Datenschutzklauseln[123] zu verwenden.

Nachdem es keine gesetzlichen Vorgaben gibt, welche das Eigentum an nicht-personenbezogenen Daten regeln, ist eine vertragliche Regelung unumgänglich, um wichtige Daten für das Unternehmen zu schützen und keinen Wettbewerbsnachteil im Falle von Datenverlusten zu erleiden. Daten sind zumeist ortslos, haben keinen eindeutigen Besitzer und können durch mehrere Personen gleichzeitig genutzt werden. Um hier eine klare Zuordnung zu schaffen, ist, soweit technisch und organisatorisch möglich, vertraglich für alle Geräte und Daten ein eindeutiger Eigentümer festzulegen. Ergänzend dazu schaffen vertragliche Regeln für den Zugriff und die Nutzung der Daten klare Verhältnisse.

Vorzugsweise sind maschinengenerierte Daten rechtlich dem Dienstleister der IIoT-Anwendung zuzuordnen, damit die Einflussnahme auf die zu verarbeitenden Daten beim

[120] *Maurer/Pollirer*, Dako 2019, 51.
[121] *European Union Agency for Cybersecurity (ENISA)*, https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot
[122] *European Union Agency for Cybersecurity (ENISA)*, https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design
[123] Datenschutz-GrundVO 2016/679 ABI L 2016/119, 49; 62; 20.

Technologie-Experten verbleibt und dieser so die Leistungsfähigkeit der IIoT-Anwendung sicherstellen kann. Die spezifische Rechtezuordnung ist dann in den individuellen Verträgen (Datennutzungsvertrag, Lizenzvertrag, Daten-Überlassungsvertrag o.Ä.) durchzuführen.[124] Das „Rechtshandbuch Industrie 4.0 und Internet of Things“[125] von Thomas Sassenberg / Tobias Faber bietet hierzu eine gute Referenz-Checkliste für die Regelegung von IoT-Verträgen.

Diese vertraglichen Handlungsempfehlungen sind nicht abschließend, sondern bieten einen Leitfaden, welcher individuell für den Einzelfall zu evaluieren, zu konkretisieren und ggfls. zu ergänzen ist.

[124] *Raffling/Schock (Hrsg)*, Digitale Wirtschaft und Industrie 4.0 (2018) 86f.
[125] *Sassenberg/Faber*, Rechtshandbuch Industrie 4.0 und Internet of Things – Praxisfragen und Perspektiven der digitalen Zukunft (2017) 1ff.

# 5 Haftungsfragen im digitalen Binnenmarkt

Die vorhergehenden Kapitel haben einen groben Überblick über die wichtigsten europarechtlichen Rahmenbedingungen für den Einsatz von IIoT-Anwendungen, sowohl für die Hersteller, als auch Nutzer gegeben. Bislang unberücksichtigt gelassen wurden die in diesem Zusammenhang möglichen Haftungsfragen im digitalen Binnenmarkt.

Der nachfolgende Abschnitt setzt sich mit den zu erwartenden Rechtsfolgen bei Haftungsfragen im Zusammenhang mit dem Einsatz von IIoT-Anwendungen auseinander. An den anschließenden Beispielen lassen sich bereits einige Haftungsfragen ableiten:

- Wer haftet bei Störungen oder Cyberangriffen auf IIoT-Systeme?
- Wer haftet, wenn sensible personenbezogene oder vertrauliche nicht-personenbezogene Daten verloren gehen?
- Wer haftet bei Maschinen- oder Personenschäden aufgrund von fehlerhaften Daten oder Fehlhandlungen durch automatisierte intelligente Geräte oder IIoT-Anwendungen?
- Wer haftet bei fehlerhaften Auswertungen/Analysen von Daten? Ist eine solche Falschinformation schon ausreichend, um den Tatbestand der Irreführung von Nutzern der IIoT-Anwendung zu erfüllen?
- Wer haftet bei Schäden an Produkten, welche ursächlich auf IIoT-Anwendungen zurückzuführen sind?
- Wer haftet bei automatisierten Fehlhandlungen durch den Einsatz von KI-Systemen?

Durch die Verwendung von IIoT-Anwendungen in industriellen Produktionsanlagen unterwerfen sich sowohl Hersteller, als auch Nutzer dieser Systeme einer gewissen Rechtsunsicherheit (Fehler, Haftung, Beweislast, Durchsetzbarkeit von Ansprüchen, etc.) oder sind sogar einem Kontrollverlust ausgesetzt, sofern keine dezidierten vertraglichen Regelungen zwischen den Parteien bestehen.

Dieser Abschnitt gibt einen Überblick über die aktuelle europäische Rechtslage und begründet einen möglichen Reformbedarf bei Haftungsthemen im digitalen Binnenmarkt. Die Fragen, welche die einzelnen nationalen Produkthaftungsrechte betreffen und die europarechtlichen Vorschriften ergänzen, werden in diesem Rahmen offengelassen und nicht weiter untersucht.

## *5.1 Haftungsrechtliche Herausforderungen in Zusammenhang mit IIoT-Anwendungen in der Europäischen Union*

Wer kennt die alltäglichen Situationen in der industriellen Produktion nicht, wenn ein Produktionsprozess aufgrund eines Fehlverhaltens eines digitalen Produktes (z.B. Software, IIoT-Anwendung) nicht ordnungsgemäß funktioniert und möglicherweise aufgrund dieser Fehlfunktion Anlagen nicht produzieren können, Fehlteile produziert werden oder ein Schaden am Endprodukt entsteht. Viele Unternehmen haben mit diesen Herausforderungen zu kämpfen und stellen sich die berechtigte Frage, wer für die Folgeschäden aufkommt und welche rechtlichen Möglichkeiten es gibt Ansprüche geltend zu machen.

Ein ausgewogenes Haftungsrecht ist sowohl im Sinne der Hersteller, als auch der Verbraucher wichtig, um einer möglichen vermehrten finanziellen Auslagerung von Haftungsrisiken auf Versicherungen vorzubeugen. Je höher das Risiko einer möglichen Haftung für einen Hersteller mit seinem Produkt ist, desto höher ist womöglich der Preis des Produktes, da mit der Risikoabwälzung durch den Kostenausgleich dieses Risiko wieder kompensiert werden soll. Im Umkehrschluss würde dadurch ein unausgeglichener Wettbewerb im EU-Binnenmarkt entstehen, da Produkte mit einem geringen Risiko fehlerhaft zu werden, günstiger am Markt angeboten werden können. Damit das Haftungsrisiko minimiert wird, ist „ein Produkt das Sicherheit bietet“ (Art. 6 Abs. 1 RL 85/374/EWG) ein Kernkriterium für das fehlerfreie Produkt und somit ein wichtiger Innovationstreiber am Markt.[126]

Bevor die europarechtlichen Rechtsgrundlagen untersucht werden, folgt ein Exkurs zum österreichischen Zivilrecht, um kurz auf die Grundlagen des Haftpflichtrechts einzugehen. Es wird prinzipiell zwischen zwei Arten rechtlicher Haftung differenziert. Einerseits der vertraglichen Haftung, bei der sich die Schadenshaftung aus dem Vertragsverhältnis zwischen den Parteien ergibt und andererseits der außervertraglichen Haftung, bei der Haftungsfragen außerhalb eines Vertrags geklärt werden (Produkthaftung).

[126] *Verbraucherzentrale Bundesverband (vzbv)*, "Safety by Design"-Produkthaftungsrecht für das Internet der Dinge / Diskussionspapier der Verbraucherzentrale Bundesverbands (vzbv) zur Evaluierung der europäischen Produkthaftungsrichtlinie (85/374/EWG) (2017) 3.

Im B2B-Bereich im Anlagen- und Maschinenbau sind vertraglich vereinbarte Haftungsbedingungen durchaus üblich. Dabei stehen Haftungsbeschränkungen und die spezifische Ausgestaltung der Mängelhaftung (Gewährleistung) im Vordergrund. Sind Schäden an Produkten auf IIoT-Anwendungen zurückzuführen, so ist im Sinne der außervertraglichen Haftung das Produkthaftungsgesetz anzuwenden.

Gemäß dem österreichischen Schadenersatzrecht (=Haftpflichtrecht) im ABGB (u.a. §1311 ABGB, §1295 ABGB) sind die zu prüfenden Elemente Schaden, Kausalität, Rechtswidrigkeit und Verschulden Voraussetzung für die Erfüllung der Verschuldenshaftung und eines möglichen Schadenersatzanspruches.

Das österreichische Schadensersatzrecht ist somit als verschuldensabhängige Haftung ausgestaltet.

## *5.2 Produkthaftungsrichtlinie*

Bereits seit dem Jahre 1985 ist innerhalb der europäischen Wirtschaftsgemeinschaft die Produkthaftungs-RL 85/374/EWG gültig und wurde seitdem bis auf „die Erweiterung des Anwendungsbereichs auf unverarbeitete Landwirtschaftliche Erzeugnisse“[127] unverändert belassen. Anwendung findet die Richtlinie auf alle beweglichen „Produkte“ (einschließlich Elektrizität) unter Berücksichtigung einiger Ausnahmen (u.a. „landwirtschaftliche Naturprodukte“).[128] Umgesetzt und erweitert wird diese europäische Richtlinie durch diverse nationale Gesetze in den einzelnen Mitgliedstaaten.

### 5.2.1 Anwendung der Richtlinie auf IIoT-Anwendungen

Ob eine IIoT-Anwendung als „bewegliche Sache“ einzuordnen ist und in den Anwendungsbereich der Produkthaftungsrichtlinie fällt, ist äußerst fraglich und eher mit nein zu beantworten, da es sich hierbei vielmehr um eine Dienstleistung bzw. Softwareanwendung handelt. Bei IIoT-Produkten können das Produkt, die digitale Dienstleistung und die Daten

[127] Richtlinie 1999/34/EG des Europäischen Parlaments und des Rates vom 10. Mai 1999 zur Änderung der Richtlinie 85/374/EWG des Rates zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte ABI L 1999/141, 20.
[128] Richtlinie des Rates vom 25.Juli 1985 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte (85/374/EWG) ABI L 1985/210, 29.

zumeist nicht unabhängig voneinander funktionieren und sind teilweise integriert, weshalb das Produkthaftrecht aufgrund der zunehmenden Digitalisierung zukünftig auch digitale Dienstleistungen und Daten als Regelungsgegenstand einschließen sollte.[129]

Eine IIoT-Softwareanwendung, wie beispielsweise Condition Monitoring oder Predictive Maintenance, verarbeitet Daten, analysiert diese und trifft Vorhersagen bzw. setzt Aktionen an der Maschine oder Anlage des Kunden der Anwendung. Im Zuge dieses Prozesses können Daten verloren gehen (hier ist zwischen personenbezogenen und nicht-personenbezogenen Daten zu differenzieren) oder werden fehlerhaft an den Nutzer/Kunden ausgegeben.

Fehlerhaft gelieferte Daten stellen grundsätzlich einen Mangel der IIoT-Anwendung dar. Der Kunde hat deshalb, abhängig vom Vertragsverhältnis, die Möglichkeit Gewährleistungsansprüche geltend zu machen. In B2B-Verträgen, welche nicht den jeweiligen nationalen Konsumentenschutzregulierungen unterliegen, besteht die Möglichkeit Gewährleistungsansprüche einzuschränken oder auszuschließen (Österreich: außer es ist der Tatbestand der Sittenwidrigkeit erfüllt). Bestehen keine vertraglichen Einschränkungen der Gewährleistung, dann ist in jedem Fall gemäß den einzelstaatlichen Gewährleistungsregulierungen (Österreich: ABGB ; Deutschland: BGB) zu prüfen, welche Gewährleistungsbehelfe bzw. Abhilfemaßnahmen zur Verfügung stehen und wie die Wiederherstellung von verloren gegangenen oder fehlerhaften Daten überhaupt möglich ist. Es ist davon auszugehen, dass in vielen Streitfällen eine Nachbesserung, Korrektur oder Wiederherstellung der ursprünglichen Datensätze technisch nicht mehr möglich ist. Folgend ist im Einzelfall zu beurteilen, ob dem Geschädigten möglicherweise Schadensersatzansprüche im Fall eines Gewinnentgangs bei Produktionsausfällen, bei diversen Folgeschäden oder bei Datenverlust zustehen. Um zuvor genannte Haftungsrisiken zu minimieren ist es daher in B2B-Geschäften möglich vertragliche Einschränkungen vorzunehmen. Anders ist es, wenn anwendbares deutsches Recht vereinbart ist, denn in diesem Fall ist es aufgrund des zweifelsfrei strengeren AGB-Rechts (gemäß § 307 BGB Inhaltskontrolle) so, dass Haftungsausschlüsse bzw. Haftungsbeschränkungen aufgrund des wesentlichen Abweichens von der gesetzlichen Regelung, bei Standardverträgen nicht mit dem deutschen Recht vereinbar

[129] *Verbraucherzentrale Bundesverband (vzbv)*, "Safety by Design"-Produkthaftungsrecht für das Internet der Dinge / Diskussionspapier der Verbraucherzentrale Bundesverbands (vzbv) zur Evaluierung der europäischen Produkthaftungsrichtlinie (85/374/EWG) (2017) 4.

sind. Diese Restriktion von Ausschlüssen oder Beschränkungen der Haftung im deutschen Recht, gilt unabhängig davon ob der Kunde diese akzeptiert oder nicht.[130]

Handelt es sich bei den fehlerhaften oder verloren gegangenen Daten um personenbezogene Daten, so ist gemäß der DSGVO eine unverzügliche Meldung der Datenschutzverletzung durchzuführen. Diese Meldung ist vom Auftragsverarbeiter (IIoT-Hersteller) an den Verantwortlichen (in unserem Beispiel ist das der Nutzer bzw. Kunde) durchzuführen, sofern dieser die Verletzung festgestellt hat (Art. 33 Abs. 2 DSGVO). Außerdem ist die Datenschutzverletzung vom Verantwortlichen (Art. 33 Abs. 1 DSGVO) an die zuständige Aufsichtsbehörde (Art. 55 DSGVO) zu melden.

Weiters ist gemäß Art. 34 DSGVO die von der Datenschutzverletzung betroffene Person unverzüglich zu benachrichtigen (sofern keine Ausnahmebedingung laut Art. 34 Abs. 3 erfüllt ist, welche eine Benachrichtigung nicht erforderlich macht).

Bei einer Verletzung des Schutzes von personenbezogenen Daten hat die geschädigte Person, unter der Voraussetzung, dass „aufgrund des Verstoßes gegen die DSGVO, ein materieller oder immaterieller Schaden entstanden ist, das Recht Schadenersatzansprüche gegenüber dem Verantwortlichen oder dem Auftragsverarbeiter geltend zu machen".[131] Um einen Schadenersatzanspruch abzuwehren, muss der Verantwortliche oder der Auftragsverarbeiter gemäß Art. 82 Abs. 3 DSGVO nachweisen, dass die Verantwortung für den Schadenseintritt nicht bei ihnen liegt. Inwieweit diese Beweislastpflicht infolge einer Datenschutzverletzung praxistauglich ist, wird sich erst mit der steigenden Anzahl an Datenschutzverletzungen zeigen.

Die Regelungen für die Verhängung von Geldbußen bei Datenschutzverletzungen sind folgend in Art. 83 DSGVO geregelt.

Gemäß Art. 1 RL 85/374/EWG haftet „der Hersteller des Produktes für den Schaden, welcher durch einen Fehler dieses Produktes verursacht worden ist".[132] Übereinstimmend mit der österreichischen Regelung im ABGB ist neben dem Fehler und dem Schaden auch der kausale ursächliche Zusammenhang für die Haftung maßgebend (Art. 4). Der Nachweis für die

[130] *Bräutigam/Klindt*, Digitalisierte Wirtschaft / Industrie 4.0 (2015) 81f.
[131] Datenschutz-GrundVO 2016/679 ABI L 2016/119, 81.
[132] ProdukthaftungsRL 85/374/EWG ABI L 1985/210, 30.

Kausalität zwischen dem Fehler und dem Schaden ist durch den Geschädigten zu erbringen. Aufgrund des erheblichen Aufwands (Kosten, Zeit) für den Nachweis und der oft spärlichen technischen Informationen über das in Frage stehende Produkt, stellt es für den Geschädigten zumeist eine Hürde dar, einen möglichen Schadenersatzanspruch geltend zu machen.[133] Im Unterschied zur Verschuldenshaftung (Rechtswidrigkeit und Verschulden) im ABGB ist unter Berücksichtigung der Ausnahmen der Herstellerhaftung gemäß Art. 7, die Richtlinie selbst als verschuldensunabhängige Haftung ausgestaltet.

### 5.2.2 Produkthaftung bei IIoT-Anwendungen anhand eines Beispiels

Bleiben wir in unserem Beispiel beim Automobilzulieferer, welcher in diesem Fall durch Industrieöfen wärmebehandelte Karosserieteile (zur Erhöhung der Sicherheit von PKW's durch Verbesserung der Bauteileigenschaften Festigkeit und Steifigkeit, u.a. durch den Einsatz von IIoT-Anwendungen) herstellt, welche nachfolgend in PKW's verbaut werden. Bei einem Verkehrsunfall kommt eine Person mit dem PKW von der Straße ab und prallt gegen ein Hindernis. Die speziell auf eine verbesserte Crash-Performance optimierten Karosserieteile hielten dem Aufprall nicht stand und die Person wurde schwer verletzt. Die Gerichte müssen nun klären, ob das Fahrzeug sicher war, die Karosserie ordnungsgemäß berechnet und die Qualitäts- und Sicherheitsstandards entsprechend dem aktuellen Stand der Technik erfüllt (d.h. gefertigt bzw. wärmebehandelt) wurden.

Dieses Beispiel macht deutlich welches Ausmaß die Produkthaftung erreichen kann und welche möglichen Konsequenzen dem Hersteller drohen können.

Der Hersteller haftet nicht, wenn er beweisen kann, dass eine der in Art. 7 festgelegten Ausnahmen zutrifft. Hierfür kommt es darauf an, ob „der Fehler nicht vor schon vorlag, als das Produkt in Verkehr gebracht wurde (Art. 7 lit b) oder der Fehler darauf zurückzuführen ist, dass das Produkt verbindlichen hoheitlich erlassenen Normen entspricht (Art. 7 lit d) oder der Fehler nach dem technischen Wissensstand zum Zeitpunkt des Inverkehrbringens nicht erkannt werden konnte (Art. 7 lit e) oder es sich um den Hersteller eines Teilproduktes handelt und der Fehler durch die Konstruktion des Produktes, in welches das Teilprodukt eingearbeitet

[133] Bericht der Kommission an das Europäische Parlament, den Rat und den Europäischen Wirtschafts- und Sozialausschuss über die Anwendung der Richtlinie des Rates zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte (85/374/EWG), COM(2018) 246 final (2018) 6.

wurde hervorgerufen wurde oder durch die Anleitungen des Herstellers des Produktes verursacht worden ist (Art. 7 lit f).“[134]

Gemäß Art. 15 Abs. 1 lit b können die Mitgliedstaaten vom zuvor zitierten Art. 7 lit e in dem Sinn eine abweichende nationale Rechtsvorschrift erlassen, in welcher der Hersteller des Produktes trotz Nachweises des technischen Wissenstandes zum Zeitpunkt des Inverkehrbringens haftbar bleibt.

Die Richtlinie 85/374/EWG hat nun über Jahrzehnte hinweg ihren Zweck, trotz der industriellen Revolutionen, erfüllt und seinen Teil zur Verwirklichung des EU-Binnenmarktes beigetragen. In Bezug auf Industrie 4.0 Produkte und Dienstleistungen ist bezugnehmend auf diese Richtlinie nicht geklärt, wie zwischen einem Produkt und einer Dienstleistung im Sinne dieser Richtlinie differenziert wird. Um den gewachsenen Anforderungen eines dynamischen digitalen Binnenmarktes gerecht zu werden, wäre laut Meinung der Europäischen Kommission ein erster Schritt, die Terminologien wie z.B. „Fehler“, „Schaden“ oder „Hersteller“ den neuen Gegebenheiten der digitalen Welt anzupassen.[135]

Wie zuvor ausgeführt, schreibt der Art. 4 RL 85/374/EWG vor, dass die Geschädigten in der Pflicht sind die Kausalität des Schadens zum Fehler zu beweisen. Legt man diese Nachweispflicht auf digitale IIoT-Anwendungen wie zum Beispiel Condition Monitoring um, dann wird es für die Nutzer dieser Systeme zunehmend schwieriger, einen Zusammenhang zwischen dem Fehler und dem Schaden festzustellen, geschweige denn zu beweisen.

Im Diskussionspapier des *Verbraucherzentrale Bundesverbands* wird vorgeschlagen, dass in der Folge von Fehlern (z.B. Fehlentscheidungen autonomer digitaler Systeme oder Probleme in der Kommunikation) von digitalen IIoT-Systemen die Nutzer von der Nachweispflicht insofern befreit werden sollen, sodass vom Nutzer nur die Funktionsfähigkeit des Geräts beurteilt wird.[136]

[134] ProduktHaftungsRL 85/374/EWG ABI L 1985/210, 31.
[135] *Europäische Kommission*, Bericht der Kommission COM(2018) 246 final (2018) 9.
[136] *Verbraucherzentrale Bundesverband (vzbv)*, "Safety by Design"-Produkthaftungsrecht für das Internet der Dinge / Diskussionspapier der Verbraucherzentrale Bundesverbands (vzbv) zur Evaluierung der europäischen Produkthaftungsrichtlinie (85/374/EWG) (2017) 3.

Als möglicher Entlastungsnachweis bei Haftungsfragen und zur Minimierung des Haftungsrisikos (Produkte und Dienstleistungen werden durch die Orientierung am Stand der Technik sicherer) ist die Einhaltung von internationalen Standards und Normen (im Bereich von IIoT allen voran IT-Sicherheitsstandards) von hoher Bedeutung.

### 5.2.3 Haftungsfragen beim Einsatz von KI-Systemen

Die nächste Entwicklungsstufe von IIoT-Anwendungen sind digitale Systeme, welche KI-Algorithmen einsetzen, die weitgehend autonom agieren und somit sowohl für den Hersteller als auch für den Nutzer solcher Anwendungen noch intransparenter und unkontrollierbarer werden.

Die EU-Kommission hat in ihrer neuesten Stellungnahme KI wie folgt definiert: "Künstliche Intelligenz bezeichnet Systeme mit einem 'intelligenten' Verhalten, die ihre Umgebung analysieren und mit einem gewissen Grad an Autonomie handeln, um bestimmte Ziele zu erreichen."[137]

Künstliche Intelligenz wird bei IIoT-Anwendungen vorrangig dafür eingesetzt, um auf Basis von Daten, Trends und Erfahrungswerten von Maschinen und Anlagen, durch automatisierte Handlungen (z.B. Änderung von Prozessparametern) mögliche Prozesse zu optimieren, dadurch Kosteneinsparungen zu erreichen und die Qualität von Produkten zu verbessern. Im Anwendungsbereich von Instandhaltungs- und Wartungsassistenten werden durch automatisierte Vorgänge, z.B. Ersatzteile, automatisch bei vorab definierten Herstellern nachbestellt (Gefahr von Lock-In-Effekten). Manche autonomen Systeme gehen soweit und wählen die Hersteller auf Basis von Echtzeit-Vergleichsangeboten aus (z.B. bester Preis und kürzeste Lieferzeit). Die tagesaktuellen Daten werden entweder aus dem Internet oder von internen Plattformen der Unternehmen bezogen. Diese Nachbestellungen erfolgen nicht erst, wenn die Teile defekt sind, sondern werden aufgrund von vorausschauenden Trendanalysen und Erfahrungswerten rechtzeitig nachbestellt, bevor diese Teile überhaupt defekt werden, um so Maschinen- und Anlagenstillstände zu vermeiden.

[137] *Europäische Kommission*, Mitteilung der Kommission COM (2018) 237 final, 1.

Automatische Nachbestellungen durch intelligente Industrie 4.0-Anwendungen verlangen einen Vertragsabschluss durch eine Willenserklärung. Nach geltendem deutschem Recht können Willenserklärungen per se nur von Menschen abgegeben werden.[138]

Demzufolge können autonome IIoT-Systeme keine Willenserklärung abgeben, sondern werden nur als Hilfsmittel für die Formulierung dieser genutzt. Es ist ähnlich wie die Handhabung eines Kugelschreibers zu verstehen, der als Tool genutzt wird, um das vom Menschen gewollte wiederzugeben (dies passiert nicht eigenständig).

Um diese Fragen hinsichtlich KI-Systemen eindeutig beantworten zu können, bedarf es einer weiteren Untersuchung einer sicherheitsrelevanten Fehlentscheidung aufgrund einer autonomen Handlung eines IIoT-Systems, mit der Konsequenz eines Produktfehlers, anhand des bereits zuvor dargelegten Art. 7 lit e RL 85/374/EWG. Ungeachtet einer Feststellung der Kausalität, wird es nach Art. 7 lit e RL 85/374/EWG nicht möglich sein zu belegen, dass der Fehler schon zum Zeitpunkt des Inverkehrbringens bestanden hat. Neben vielen offenen Haftungsfragen stellt bei digitalen Anwendungen die Beweisführung eine große technische und rechtliche Herausforderung dar.[139] Wer haftet im Fall von Maschinen- oder Personenschäden, welche durch IIoT-Anwendungen verursacht worden sind?

Unabhängig davon, ob ein autonomes IIoT-System eingesetzt wird oder nicht, hat der Schutz des IIoT-Systems und der verarbeiteten Daten höchste Priorität. Datensicherheit, ist im Sinne von IT-Sicherheit infolge der fortschreitenden Vernetzung und enormen Datenmengen von großer Bedeutung für Hersteller und Nutzer von IIoT-Systemen. Für ein produzierendes Unternehmen hätte ein Ausfall der Produktion, ein Eingriff in die Produktion oder ein Datenverlust aufgrund eines Cyberangriffs auf das IIoT-System womöglich schwerwiegende Folgen.

### 5.2.4 Produktsicherheit

Die EU-Produktsicherheitsrichtlinie 2001/95/EG, welche nicht auf Produkte im B2B-Bereich anwendbar ist, legt Sicherheitsanforderungen für Produkte fest, welche gewährleisten sollen,

[138] https://www.noerr.com/de/newsroom/news/kuenstliche-intelligenz-wenn-roboter-vertraege-schliessen
[139] *Verbraucherzentrale Bundesverband (vzbv)*, "Safety by Design"-Produkthaftungsrecht für das Internet der Dinge / Diskussionspapier der Verbraucherzentrale Bundesverbands (vzbv) zur Evaluierung der europäischen Produkthaftungsrichtlinie (85/374/EWG) (2017) 10.

„dass erstmals auf den Markt gebrachte Produkte sicher sind“[140]. Beim in Verkehr bringen von Maschinen und Anlagen legt die erforderliche Einhaltung der europäischen Maschinenrichtlinie 2006/42/EG einen angemessenen Sicherheitsmaßstab fest.

Die Einhaltung von IT sicherheitstechnischen Anforderungen werden vorwiegend von den nationalen Produktsicherheitsgesetzen geregelt. Im Bereich der Produkthaftung ist aufgrund der sehr vagen Rechtsvorschriften unsicher, wie ohne zusätzliche vertragliche Regelung die Einhaltung von geforderten IT Sicherheitsstandards im B2B-Bereich sichergestellt werden kann.[141] In Übereinstimmung mit der Maschinenrichtlinie 2006/42/EG, würde bei einer nicht Erfüllung der IT Sicherheitsanforderungen, möglicherweise eine Gefährdungshaftung vorliegen.

In diesem Zusammenhang sind auf Grundlage der Produkthaftungsrichtlinie 85/374/EWG und der EU-Produktsicherheitsrichtlinie 2001/95/EG, die nationalen Gesetzgeber gefordert, die Sicherheitsanforderungen für IT-Systeme zu definieren. Damit ein umfassendes IT Sicherheitsumfeld realisiert werden kann, sind neben dem Produkthersteller auch die Nutzer/Kunden dazu angehalten, die entsprechenden IT-Maßnahmen umzusetzen, um ein sicheres IT-Umfeld für die Nutzung von IIoT-Systemen bereitzustellen.

Die Implementierung von State-of-the-Art Sicherheitskonzepten, um unerlaubten Zugriff und Missbrauch von Daten vorzubeugen und die Verpflichtung entsprechende Zertifizierungen von Produkten vor dem ersten in Verkehr bringen durchführen, würden einen gewissen Sicherheits-Mindeststandard gewährleisten. In B2B-Verträgen kann durch die Festlegung von Sicherheitsniveaus und entsprechend darauf abgestimmten Haftungsregulierungen Rechtssicherheit in Bezug auf die Produkthaftung gegeben werden.

## *5.3 Ausblick Haftungsrecht*

Innerhalb der Europäischen Union gibt es u.a. in den diversen nationalen Strategie-Plattformen bereits Überlegungen und Szenarien, wie mögliche Haftungsregulierungen für autonome digitale KI-Systeme möglichst praxistauglich ausgestaltet werden könnten.

[140] Richtlinie 2001/95/EG des europäischen Parlaments und des Rates vom 3. Dezember 2001 über die allgemeine Produktsicherheit ABI L 2002/11, 4.
[141] *Bundesministerium für Wirtschaft und Energie (BMWi)*, Industrie 4.0 – wie das Recht Schritt hält (2016) 4f.

Ein Ansatz zur Regelung der Produkthaftung für autonome Systeme ist die Umsetzung einer Gefährdungshaftung. In diesem Vorschlag könnte der Geschädigte im Falle eines Fehlers/Schadens seine Ansprüche direkt beim Betreiber bzw. Nutzer geltend machen. Dieser könnte seine Ersatzansprüche dann beim Hersteller einfordern. Eine weitere essentielle Frage ist die Behandlung von Schäden, welche erst durch das Lernergebnis des KI-Systems verursacht wurden. In diesem Zusammenhang steht eine Ausweitung des Verantwortungsbereichs auf die Programmierer oder Ingenieure dieser Software in Diskussion. Ein Ziel dieser Gefährdungshaftung ist die Anregung von Herstellern autonomer Systeme zur Ausführung der Systeme entsprechend State-of-the-Art Sicherheitsanforderungen und somit der Reduktion des Risikos eines Haftungstatbestandes aufgrund eines Fehlers/Schadens. Ein weiterer Ansatz ist die Schaffung eines Versicherungssystems, analog zum Haftpflichtsystem für Kraftfahrzeuge. Diese Variante wäre für die Geschädigten günstiger, da die Risiken einer Haftung minimiert werden bzw. auf die Versicherung abgewälzt werden können. Im Umkehrschluss ist zu erwarten, dass aufgrund dieses etablierten „Fangnetzes" die Investitionen in die Weiterentwicklung von Produkten der Hersteller nachlassen werden.[142]

[142] *Reinisch*, ÖJZ 2019, 303f.

# 6 Conclusio

Die vorangegangenen Abschnitte dieser Master Thesis haben auf Grundlage der europäischen Rechtsvorschriften, den Zusammenhang mit und die Auswirkungen auf den digitalen Binnenmarkt, insbesondere auf Industrie 4.0 Lösungen diskutiert. Zusammenfassend widmet sich dieser letzte Abschnitt der Darstellung der zentralen Ergebnisse dieser Arbeit und formuliert darauf basierend Empfehlungen, für die Bewältigung der rechtlichen Herausforderungen.

## *6.1 Zusammenfassung*

Die „vier" industriellen Revolutionen, beginnend mit der Entwicklung der Dampfmaschine bis hin zur Implementierung von Digitalisierungslösungen in der industriellen Produktion, haben auch bei der Weiterentwicklung der europäischen Rechtsvorschriften nicht Halt gemacht und diese durchaus geprägt. Der für die vollständige Verwirklichung der europäischen Idee mitunter bedeutendste Puzzlestein ist die aktuelle Entwicklung des digitalen Binnenmarktes.

Der digitale Binnenmarkt ist geprägt von enormen Datenmengen („Big Data"), umfangreicher Kommunikation zwischen den Marktteilnehmern und einem daraus resultierenden dynamischen Markt- und Wettbewerbsumfeld. Dieser digitale Marktplatz wird in der Maschinen- und Anlagenbaubranche durch die Entwicklung und den vermehrten Einsatz von Industrie 4.0- bzw. Industrial Internet of Things (IIoT)-Anwendungen genutzt. Instandhaltungs- und Wartungsanwendungen wie Condition Monitoring oder Predictive Maintenance werden dazu eingesetzt, um auf Basis von Datenanalysen Vorhersagen über mögliche Anlagenstillstände oder Komponentenausfälle zu treffen, Produktionslinien zu optimieren, Kosten zu reduzieren, die Qualität der Produkte zu verbessern und folgend die Wettbewerbsfähigkeit zu steigern.

Dieses revolutionäre Umfeld der Digitalisierung fordert in vielen Bereichen eine Überarbeitung oder Neuentwicklung von rechtlichen Rahmenbedingungen, um einem unausgeglichenen oder missbräuchlichen Wettbewerb vorzubeugen und einen funktionierenden und international wettbewerbsfähigen digitalen Binnenmarkt zu schaffen. Die Europäische Union hat für das Ziel der Realisierung eines vollkommenen Binnenmarktes

und der damit einhergehenden Harmonisierung aller Rechtsvorschriften in den einzelnen Mitgliedstaaten bereits einige Richtlinien und Verordnungen umgesetzt. Die Bedeutung der Digitalisierung für den Binnenmarkt, dem möglichen positiven Einfluss auf die Wettbewerbsfähigkeit und auf das wirtschaftliche Wachstum der EU, haben die Verantwortlichen in der Europäischen Union erkannt und darauf mit der Vorstellung zahlreicher europäischer und nationaler Zukunftsstrategien für die Gestaltung und Weiterentwicklung eines Rechtsrahmens für den digitalen Binnenmarkt reagiert.

Die Evaluierung der rechtlichen Rahmenbedingungen hat ergeben, dass seit dem Jahr 2015 bereits 28 neue Gesetzesinitiativen für die Förderung des digitalen Binnenmarktes durch die Europäische Union erfolgreich beschlossen wurden. Insbesondere spielen das Datenschutzrecht, das Urheberrecht, das Kartell- und Wettbewerbsrecht sowie die Vorschriften zur Produkthaftung für Unternehmen, die mit Industrie 4.0 als Hersteller oder Nutzer in Verbindung kommen, eine Rolle. Für den in dieser Master Thesis primär betrachteten Bereich der Industrie 4.0-Anwendungen sind demnach einige bereits umgesetzte Richtlinien und Verordnungen auf europäischer Ebene von Bedeutung. Im Ergebnis kann festgestellt werden, dass dabei vor allem die Datenschutz-Grundverordnung für die Ausführung (Design-Rules) der IIoT-Anwendungen, die Verordnung für den freien Verkehr nicht-personenbezogener Daten für Cloud-Computing Anwendungen, die Richtlinie für vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen für die Schaffung einheitlicher Gewährleistungsbedingungen und die Urheberrechtsrichtlinie für die Umsetzung von Daten-Zugangsregulierungen im digitalen Binnenmarkt wesentlich sind.

Ergänzend zu diesen neuen Rechtsvorschriften, sind auch die schon etwas ältere Produkthaftungs-Richtlinie 85/374/EWG, die Datenbankschutz-Richtlinie 96/9/EG und das primärrechtliche Kartell- und Wettbewerbsrecht Art. 101/102/103 AEUV sowie die GVO's für den digitalen Binnenmarkt von Bedeutung.

Die rechtlichen Herausforderungen für Industrie 4.0-Anwendungen im Maschinen- und Anlagenbau ergeben sich mehrheitlich aus den zuvor zitierten EU-Richtlinien und Verordnungen. Der nachfolgende Teil gibt einen Überblick über die wichtigsten Ergebnisse der im Zuge dieser Arbeit durchgeführten Rechtsinterpretation.

Die Einhaltung der Kartell- und Wettbewerbsregeln (europäisch und national) sind auch im Bereich IIoT wesentlich, um einen fairen Wettbewerb sicherzustellen. Bei der Einhaltung, aber vor allem bei der Prüfung (u.a. der Marktabgrenzung) eines möglichen Verstoßes gegen die Kartell- und Wettbewerbsvorschriften im digitalen Raum, stoßen die Wettbewerbsbehörden an ihre Grenzen.

Die rechtliche Herausforderung für den IIoT-Hersteller stellt die Verarbeitung und Verbreitung von Nutzer-Daten dar. In diesem Zusammenhang ist eine klare vertragliche Regelung über die Nutzung, Verarbeitung und Verbreitung von Daten zu treffen und auszuschließen, dass der IIoT-Hersteller durch die ihm zur Verfügung stehende Datenmenge (von verschiedensten Nutzern seiner Anwendung) eine marktbeherrschende Stellung erlangt, welche möglicherweise missbräuchlich eingesetzt werden kann.

Aus IIoT-Nutzer-Sicht sind Anwendungen so einzusetzen, dass kein Lock-In-Effekt (Bindung an Unternehmen in der vertikalen Wertschöpfungskette) entsteht. Für Unternehmen, welche eine Kooperation anstreben, besteht die Möglichkeit über den Ausnahmetatbestand gem. Art. 103 AEUV und der F&E-GVO eine rechtmäßige, für Forschungs- und Entwicklungszwecke angelegte Kooperation einzugehen.

Um zukünftig Wettbewerbsbehörden bei Verstößen ein rascheres Eingreifen zu ermöglichen, bedarf es einer Definition von einheitlichen Rahmenbedingungen für den Datenaustausch, um eine transparente Beobachtung des Marktes und das Erkennen von Veränderungen zu sicherzustellen.

Aufgrund des wirtschaftlichen Stellenwerts ist der rechtliche Schutz sowohl von sensiblen personenbezogenen Daten, als auch von nicht-personenbezogenen Daten (Maschinen- und Prozessdaten) wesentlich für die Hersteller und Anwender von IIoT-Anwendungen. Die DSGVO bietet Schutz für natürliche Personen bei der Verarbeitung personenbezogener Daten. Als Ergebnis der Betrachtung der DSGVO sind folgende grundlegenden Bestimmungen in Zusammenhang mit IIoT-Anwendungen zu beachten:
Die Anforderungen gemäß Art. 25 DSGVO „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ („privacy by design“) sind bereits bei der Umsetzung von Industrie 4.0-Anwendungen zu berücksichtigen. Im weiteren Sinne ist diese

Regulierung eine Verpflichtung sich an die aktuellen Standards und Normen zu halten (vor allem im Hinblick auf Datensicherheit und Daten-Kommunikation).[143]
Weiters ist die detaillierte Festlegung der Verantwortlichkeiten und der zu verarbeitenden Daten erforderlich. Gesetzt dem Fall es werden personenbezogene Daten verarbeitet, so ist eine Einwilligung mit der betroffenen natürlichen Person gemäß Art. 6 DSGVO abzuschließen. Ist die Verarbeitung für die Leistungserbringung der IIoT-Anwendung erforderlich, dann hat dies auf Anfrage der betroffenen Person zu erfolgen.[144]

Erfolgt die Zusammenarbeit bzw. der Austausch von personenbezogenen Daten im Rahmen eines F&E-Projekts und liegt dieses im öffentlichen Interesse, so besteht gemäß Art. 21 Abs. 6 DSGVO eine Ausnahmeregelung für die Verarbeitung dieser Daten.

Die neue „free flow of non-personal data"-Richtlinie ist angelehnt an die DSGVO, bringt aber für die Verarbeitung von nicht-personenbezogenen Daten keine wesentlichen Einschränkungen. Die Europäische Union vertraut auf die Selbstregulierung durch die Entwicklung von Verhaltensregeln. Derzeit ist es noch schwer einzuschätzen wie Unternehmen mit diesem Freiraum und dem geschenkten Vertrauen umgehen und welche Risiken oder Chancen es für den digitalen Binnenmarkt mit sich bringt. Soweit hier ein transparenter und fairer Austausch von Daten innerhalb des Binnenmarktes stattfindet und diese Daten nicht missbräuchlich verwendet werden, kann es durchaus eine Chance für die EU darstellen, um die Innovations- und Wettbewerbsfähigkeit der Unternehmen im internationalen Vergleich zu stärken.

Fortführend zum Datenschutzrecht hat die Untersuchung gezeigt, dass das Datenbankrecht nicht auf maschinengenerierte Daten, welche in IIoT-Anwendungen verarbeitet werden, anwendbar ist. Als Ergebnis der Analyse eines möglichen Schutzes von maschinengenerierten Daten als vertrauliches Geschäftsgeheimnis oder vertrauliches Know-How ist festzustellen, dass sich die Erfüllung des notwendigen Schutzbedürfnisses von Daten als geistiges Eigentum als schwierig darstellt und im Einzelfall beurteilt werden muss.

Die schon in die Jahre gekommene Produkthaftungsrichtlinie 85/374/EWG erweist noch immer ihren Dienst, müsste jedoch zeitnah an die Anforderungen des digitalen Binnenmarktes

[143] Datenschutz-GrundVO 2016/679 ABI L 2016/119, 48; 15.
[144] Datenschutz-GrundVO 2016/679 ABI L 2016/119, 36.

angepasst werden. Die Erweiterung des Anwendungsbereichs auf Softwareanwendungen und Dienstleistungen (Software-as-a-service) sowie eine Überarbeitung der Terminologien („Hersteller“, „Fehler“, „Schaden“) würden zeitgemäße rechtliche Haftungsrecht-Rahmenbedingungen für IIoT-Anwendungen schaffen.

Als Ergebnis dieser Arbeit und der Interpretation von europäischen Rechtsvorschriften in Zusammenhang mit „Industrie 4.0 / Internet of Things“ ist zusammenfassend festzustellen, dass der Rechtsrahmen für Hersteller und Kunden von digitalen Anwendungen im Maschinen- und Anlagenbau noch Gesetzeslücken aufweist, welche es erfordern, im B2B-Bereich klare vertragliche Regelungen vorzusehen, um ein adäquates Schutzniveau sowohl für die Hersteller, als auch für die Kunden sicherzustellen. Es ist anzunehmen, dass bis zur (un)möglichen Vollharmonisierung der Rechtsvorschriften für den gesamten digitalen Binnenmarkt noch viel Zeit vergehen wird. Die zahlreichen individuellen Märkte und die damit verbundenen rechtlichen Anforderungen werden sich durch die aktive Weiterentwicklung der Digitalisierung weiter verändern. Damit das Recht mit dieser sprunghaften Entwicklung Schritt halten kann, ist es notwendig, dass neben dem europäischen Gesetzgeber, vor allem die Mitgliedstaaten sowie die Normungsinstitute bzw. Zertifizierungsstellen ihren Teil dazu beitragen, geeignete Rahmenbedingungen für einen funktionierenden digitalen Raum bereitzustellen.

## *6.2 Empfehlungen*

Die rechtlichen Herausforderungen für Industrie 4.0 Instandhaltungs- und Wartungsanwendungen sind wie in dieser Arbeit ausgeführt sehr umfangreich und erfordern eine umfassende Evaluierung der eigenen Anforderungen und basierend darauf vertraglich festgelegte Rechte und Pflichten.

Die Untersuchung im Rahmen dieser Arbeit hat ergeben, dass die rechtlichen Herausforderungen der Digitalisierung vorwiegend in der Interpretation und Behandlung von Daten wiederzufinden sind.

Für IIoT-Anwendungen erfordert es deshalb eine klare Abgrenzung des Verantwortungs- und Leistungsumfangs im Vertrag. In der Vertragsgestaltung sind die Nutzungs- und

Ausschließlichkeitsrechte an den nicht-personenbezogenen und personenbezogenen Daten eindeutig festzulegen und sofern technisch überhaupt möglich eindeutig einer natürlichen oder juristischen Person zuzuordnen bzw. die Art der zu verarbeitenden Daten zu kategorisieren.

Um den Spagat zwischen dem Schutz von Daten im Sinne von Unternehmens-Know-How und der Förderung von unternehmensübergreifenden Innovationen sowie der damit verbundenen Steigerung der Wettbewerbsfähigkeit zu schaffen, erachte ich Lizenzmodelle bzw. Nutzungsrechte an Daten als eine geeignete Möglichkeit dafür.

Ein weiterer wichtiger Aspekt, der in den digitalen Strategien der Europäischen Union und der Mitgliedstaaten berücksichtigt werden muss, ist die Festlegung von einheitlichen Sicherheitsanforderungen für IT-Systeme. Die Einführung einer Richtlinie für digitale Produkte und Dienstleistungen ähnlich der europäischen Maschinenrichtlinie 2006/42/EG würde auch für IT-Systeme ein angemessenes Schutzniveau definieren und eine Kennzeichnungs- bzw. Zertifizierungspflicht für sicherheitsrelevante digitale Produkte oder Dienstleistungen einfordern. Ergänzend dazu erachte ich es als wesentlich, die Entwicklung der Normen für Industrie 4.0-Anwendungen zu fördern und als Standard in den Unternehmen zu implementieren.

Die zwingende Berücksichtigung von Normen und Standards hätte den nachhaltigen positiven Effekt, dass die derzeit bestehenden Haftungsrisiken sowohl für Hersteller als auch für Nutzer von IIoT-Anwendungen minimiert werden könnten. Die bestehenden Haftungs-Rechtsvorschriften bedarf es zu modernisieren und auf die neuen Anforderungen der digitalen Welt anzupassen. Dies kann u.a. durch die Konkretisierung der Terminologien (Hersteller, etc.), der Anpassung der Beweislast-Regulierungen (der Nachweis ist im digitalen Raum oft nicht ohne weiteres möglich) und der Erweiterung des Anwendungsbereichs der geschützten Rechtsgüter (z.B. inkludieren von Software) realisiert werden.

Im Ergebnis kann festgestellt werden, dass eine eindeutige Beantwortung der Forschungsfrage in dieser Form nur bedingt möglich ist und die Schaffung einheitlicher rechtlicher Rahmenbedingungen auf europäischer Ebene, für den digitalen Binnenmarkt, eine lohnenswerte Aufgabe für die zukünftige Untersuchungen bleibt.

# 7 Literaturverzeichnis

*Aicher*: Grundsätze und Ziele des Binnenmarktes, Grundlagen der Rechtsangleichung, Lehrgangsskript, 7. Auflage, (2018) 1ff

*Austrian Standards International - Standardisierung und Innovation*: Internet der Dinge (IoT) (letzter Zugriff: 19.11.2019)
https://www.austrian-standards.at/infopedia-themencenter/infopedia-artikel/internet-der-dinge-iot/

*Bräutigam/Klindt*: Digitalisierte Wirtschaft / Industrie 4.0, Noerr LLP, (2015) 11ff

*Bundesministerium für Wirtschaft und Energie (BMWi)*: Industrie 4.0 – Kartellrechtliche Betrachtungen, Plattform Industrie 4.0, Berlin (2018) 5ff

*Bundesministerium für Wirtschaft und Energie (BMWi)*: Industrie 4.0 – wie das Recht Schritt hält, Plattform Industrie 4.0, Berlin (2016) 4ff

*Bundesministerium des Innern / Bundesministerium für Wirtschaft und Energie / Bundesministerium für Verkehr und digitale Infrastruktur*: Legislaturbericht Digitale Agenda 2014-2017; Artikelnummer: BMI17004, Bundesregierung Deutschland, Berlin (2017) 4ff

*Ecker/Weyerstraß*: Kreative Zerstörung 4.0: Industrie 4.0 als Chance für eine stärkere Industrie, als Schlüssel für mehr Wettbewerbsfähigkeit, Wirtschaftspolitische Blätter (2016) 321ff

*Eckhardt/Höllwarth/Laux/Thiele*: Cloud & Datenschutz. Der Cloud Privacy Check (CPC), Neuerungen im europäischen Datenschutzrecht für Unternehmen, Manz'sche Verlags- und Universitätsbuchhandlung, Wien (2017) 1-17

*Ensthaler*: Industrie 4.0 und die Berechtigung an Daten, NJW 2016, 3473ff

*European Data Protection Board* (Artikel-29-Datenschutzgruppe)
(letzter Zugriff: 20.11.2019)
https://ec.europa.eu/newsroom/article29/news-overview.cfm

*Europäische Kommission*, Ein digitaler Binnenmarkt zum Nutzen aller Europäer, Factsheets (2019) 1-4

*Europäische Kommission*: Warum wir einen digitalen Binnenmarkt brauchen, Factsheets 2015, 1-3

*Europäische Kommission*: COM (2017) 9 final, Aufbau einer europäischen Datenwirtschaft, Brüssel (2017) 2ff

*Europäische Kommission*: Bericht der Kommission an das Europäische Parlament, den Rat und den Europäischen Wirtschafts- und Sozialausschuss über die Anwendung der Richtlinie des Rates zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte (85/374/EWG), COM (2018) 246 final, Brüssel (2018) 1ff

*Europäische Kommission*: Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Künstliche Intelligenz für Europa, COM (2018) 237 final, Brüssel (2018) 1ff

*Europäische Kommission*: Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Strategie für einen digitalen Binnenmarkt für Europa, COM (2015) 192 final, Brüssel (2015) 1ff

*European Union Agency for Cybersecurity (ENISA)*: Good Practices for Security of Internet of Things in the context of Smart Manufacturing
(letzter Zugriff: 20.11.2019)
https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

*European Union Agency for Cybersecurity (ENISA)*: Privacy and Data Protection by Design (letzter Zugriff: 20.11.2019)
https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

*Fraunhofer Institut für Offene Kommunikationssysteme*: ISPRAT-Studie, Cloud-Computing für die öffentliche Verwaltung, Berlin (2010) 20ff

*Gerichtshof der Europäischen Union*: Pressemitteilung Nr. 16/12, Rs C-604/10, (2012) 1f

*Graf/Križanac*: Einführung in die Datenschutz-Grundverordnung, ecolex 2017, 913

*International Organization for Standardization*: ISO/IEC 2382:2015(E), Information technology – Vocabulary, ISO copyright office, Vernier, Geneva (2015) 1ff

*Kern/Maier*: Die neue Richtlinie über digitale Inhalte und Dienstleistungen, Zak 2019, 210ff

*Maurer/Pollirer*: Der Kunde hat die Datenhoheit, Dako 2019 / 32, (2019) 50f

*Metzger*: Verträge über digitale Inhalte und digitale Dienstleistungen: Neuer BGB-Vertragstypus oder punktuelle Reform, Deutsche Juristenzeitung, 2019, 578f

*Monopolkommission (unabhängiges Beratungsgremium der deutschen Bundesregierung)*: Wettbewerbspolitik: Herausforderung digitale Märkte, Sondergutachten 68, Monopolkommission, Bonn (2015) 186f

*Noerr LLP*: Künstliche Intelligenz: Wenn Roboter Verträge schließen.
(letzter Zugriff: 23.11.2019)
https://www.noerr.com/de/newsroom/news/kuenstliche-intelligenz-wenn-roboter-vertraege-schliessen

*Österreichische Forschungsförderungsgesellschaft mbH*: Webplattform Digital Austria, Die digitale Strategie der österreichischen Bundesregierung
(letzter Zugriff: 18.11.2019)

https://www.digitalaustria.gv.at/

*Raffling/Schock (Hrsg)*: Digitale Wirtschaft und Industrie 4.0, MANZ'sche Verlags- und Universitätsbuchhandlung GmbH, Wien (2018) 2ff

*Reinisch*: Künstliche Intelligenz – Haftungsfragen 4.0 und weitere zivilrechtliche Überlegungen zu autonomen Systemen, ÖJZ 2019, 303f

*Rusche/Demary*: Zwischen Kooperation und Wettbewerb: Industrie 4.0 und europäisches Kartellrecht, IW-Report No. 14/2017, Institut der deutschen Wirtschaft (IW), Köln (2017) 7ff

*Sassenberg/Faber*: Rechtshandbuch Industrie 4.0 und Internet of Things – Praxisfragen und Perspektiven der digitalen Zukunft, C.H.BECK München (2017) 1ff

*Škorjanc*: M2M-Kommunikation: Welches Datenschutzregime ist anwendbar? Ante portas zur Anwendbarkeit der ePrivacyVO auf M2M-Dienste, ipCompetence 2018 H 20, (2018) 26

*Staudegger*: Die VO (EU) 2018/1807: Ein Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union, jusIT 2019, 8f

*Staudegger*: Die Realisierung des Digitalen Binnenmarkts - aktuelle Entwicklungen des IT-Rechts im Überblick, jusIT 2019, 1ff

*Synek/Feldmann/Herweg/Rauen*: Predictive Maintenance, Service der Zukunft – und wo er wirklich steht, Roland Berger GmbH, München (2017) 3ff

*Verbraucherzentrale Bundesverband e.V.*: "Safety by Design"-Produkthaftungsrecht für das Internet der Dinge / Diskussionspapier der Verbraucherzentrale Bundesverbands (vzbv) zur Evaluierung der europäischen Produkthaftungsrichtlinie (85/374/EWG), Verbraucherzentrale Bundesverband e.V., Berlin (2017) 3ff

*Wiebe*: Wem gehören maschinengenerierte Daten? ecolex 2017, 783-786