PAiCE

KOLLABORATIVE WERTSCHÖPFUNGS-SYSTEME IN DER INDUSTRIE

GESCHÄFTSMODELLENTWICKLUNG UND RECHTLICHE FRAGEN

iit-Institut für Innovation und Technik
in der VDI/VDE Innovation + Technik GmbH
Steinplatz 1
10623 Berlin

Impressum

Herausgeber
Begleitforschung PAiCE
iit – Institut für Innovation und Technik in der
VDI / VDE Innovation + Technik GmbH
Steinplatz 1
10623 Berlin
gabriel@iit-berlin.de
www.paice.de

Autoren
Karsten U. Bartels
Susanne Beck
Birgit Buchholz
Matthias Bürger
Sebastian Straub

Gestaltung
Loesch*Hund*Liepold
Kommunikation GmbH
Hauptstraße 28 | 10827 Berlin
paice@lhlk.de

Stand
August 2020

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Inhalt

Einleitung

Mit dem Technologieprogramm „PAiCE (Platforms|Additive Manufacturing|Imaging|Communication|Engineering) des Bundesministeriums für Wirtschaft und Energie (BMWi) wurden zukunftsweisende digitale Technologien zur Integration in industrielle Prozesse und Anwendungen gefördert. Ziel war es, Deutschlands Spitzenstellung als hochwertigen Produktionsstandort und als Anbieter für modernste Produktionstechnologien weiter zu stärken. Das Programm des BWMi ist ein weiterer Meilenstein bei der Umsetzung des Zukunftsprojekts Industrie 4.0 im Rahmen der Digitalen Agenda der Bundesregierung.

In den 17 geförderten PAiCE-Projekten wurden neue Lösungsansätze entwickelt und erprobt, die neben technischen Innovationen auch neue kollaborative Wertschöpfungssysteme umfassen. Insgesamt über 100 Unternehmen und Organisationen aus Wirtschaft und Wissenschaft erarbeiteten in den einzelnen Projekten Anwendungen in den Clustern Additive Fertigung, Engineering von Fertigungsanlagen, Kommunikation in Industrieumgebungen, autonome und dezentrale Logistik sowie Service-Robotik. Die Konsortien beschäftigten sich in praxisnahen Pilotprojekten mit der Erprobung neuer Digitaltechnologien sowie mit Fragestellungen und Herausforderungen des Technologietransfers und der Verwertung: Was hat tatsächlich Bestand in der Praxis? Wo muss noch Forschungs- und Entwicklungsarbeit geleistet werden? Was kann schon in Standards und Normen umgesetzt werden? Welche neuen Geschäftsmodelle lassen sich realisieren und wie sehen die Wertschöpfungsmodelle der Zukunft aus? Welche rechtlichen Implikationen gibt es zum Beispiel bei Haftung und Datenschutz? Bei diesen und weiteren Fragestellungen leistete die Begleitforschung projektspezifische sowie projektübergreifende Unterstützung im Rahmen der Fachgruppen „Kooperative Geschäftsmodelle für digitale Plattformen“ und „Rechtliche Herausforderungen beim Einsatz kollaborativer Systeme in der Industrie“.

Bereits in der Auftaktveranstaltung der Begleitforschung im September 2017 wurde die Notwendigkeit einer engen Verknüpfung der beiden Fachgruppen Geschäftsmodelle und Recht erkannt, was die Durchführung von gemeinsamen Workshops zur Folge hatte. Ergebnis ist diese gemeinsame Veröffentlichung in Form eines Leitfadens, der die Erfahrungen, Erkenntnisse und Ergebnisse der Arbeit beider Fachgruppen zusammenfasst. Ziel des Leitfadens ist eine Sensibilisierung der Leserinnen und Leser für die Notwendigkeit einer frühzeitigen Auseinandersetzung mit rechtlichen Aspekten bei der Entwicklung und Umsetzung kollaborativer Wertschöpfungssysteme. Diese sollte bereits mit der Ideengenerierung für zukünftige Geschäftsmodelle beginnen.

In Kapitel 1 wird zu Beginn zunächst erläutert, was genau unter kollaborativen Wertschöpfungssystemen und Geschäftsmodellen verstanden wird. Zur Veranschaulichung werden insgesamt vier kollaborative Wertschöpfungssysteme als generische Fallbeispiele vorgestellt, die sich an den Clustern der PAiCE-Projekte orientieren. Die darauf folgenden Ausführungen zum iterativen Vorgehen und zu den Herausforderungen bei der Entwicklung kollaborativer Geschäftsmodelle (Kapitel 2) und den rechtlichen Rahmenbedingungen zu deren Umsetzung (Kapitel 3) sind auf die generischen Beispiele ausgerichtet und basieren auf Erfahrungen aus den Workshops mit den PAiCE-Projekten. Im Anhang des Leitfadens finden sich zudem Checklisten für die Erarbeitung kollaborativer Geschäftsmodelle und die dabei zu klärenden rechtlichen Fragestellungen.

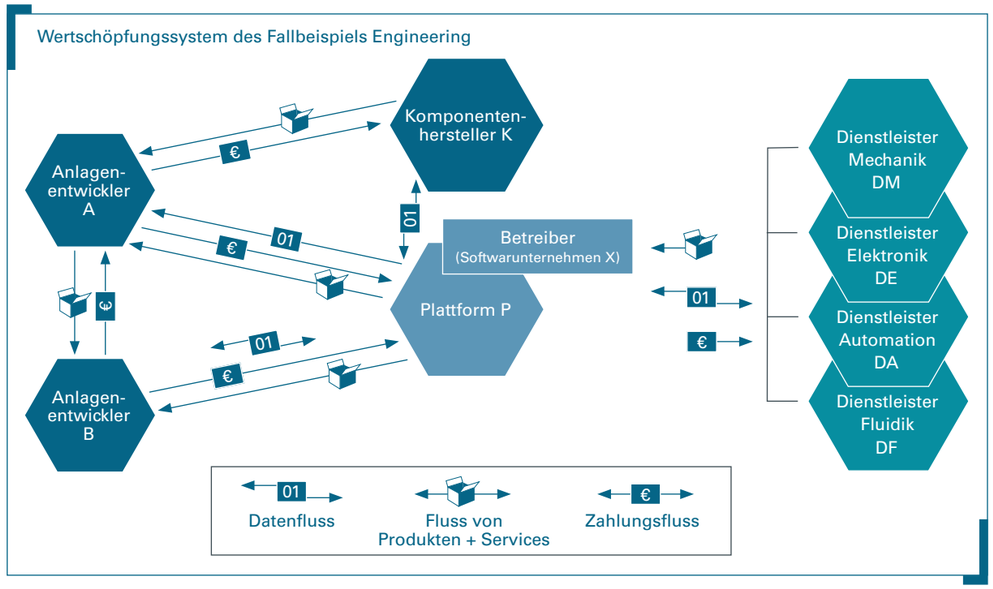
1 Kollaborative Geschäftsmodelle

Im Zuge der Digitalisierung und Globalisierung der Wirtschaft haben sich nicht zuletzt auch Produktions- und Innovationsprozesse zum Teil grundlegend gewandelt. Neue Wertschöpfungsformen sind entstanden, die nicht mehr nur unternehmensintern ablaufen und hierarchisch organisiert sind. Vielmehr werden heute vielfach verschiedene autonome Akteursgruppen über Netzwerke in die Wertschöpfung eingebunden. Unter kollaborativen Wertschöpfungssystemen werden im Folgenden insbesondere unternehmensübergreifende und vernetzte Wertschöpfungsprozesse verstanden. Die darauf aufbauenden Geschäftsmodelle können von einem einzelnen Unternehmen oder von einem Konglomerat von Unternehmen und/oder anderen Akteursgruppen entwickelt werden. Letztere werden im vorliegenden Leitfaden als kollaborative Geschäftsmodelle bezeichnet. Kollaborative Geschäftsmodelle zeichnen sich dabei insbesondere dadurch aus, dass sie

- auf zusammen erarbeiteten Wertschöpfungssystemen basieren und
- von mindestens zwei nicht miteinander verbundenen Unternehmen und/oder anderen Akteursgruppen entwickelt wurden.

Bevor im folgenden Kapitel auf die Besonderheiten der Entwicklung kollaborativer Geschäftsmodelle eingegangen wird, sollen zunächst verschiedene kollaborative Wertschöpfungssysteme in der Industrie beleuchtet werden. Die wohl bekannteste Form kollaborativer Wertschöpfungssysteme bilden Plattform-Geschäftsmodelle, die sich in vielfältigen Ausprägungen sowohl im B2C- als auch im B2B-Bereich etabliert haben. Nachfolgend werden vier kollaborative B2B-Wertschöpfungssyseme exemplarisch vorgestellt.

Engineering



Im Zentrum dieses Wertschöpfungssystems steht eine Entwicklungs-Plattform, die zunächst anlagenbetreibende und anlagenentwickelnde Unternehmen zusammenführt und diesen dann durch verschiedene Dienstleistungen einen zusätzlichen Mehrwert bietet.

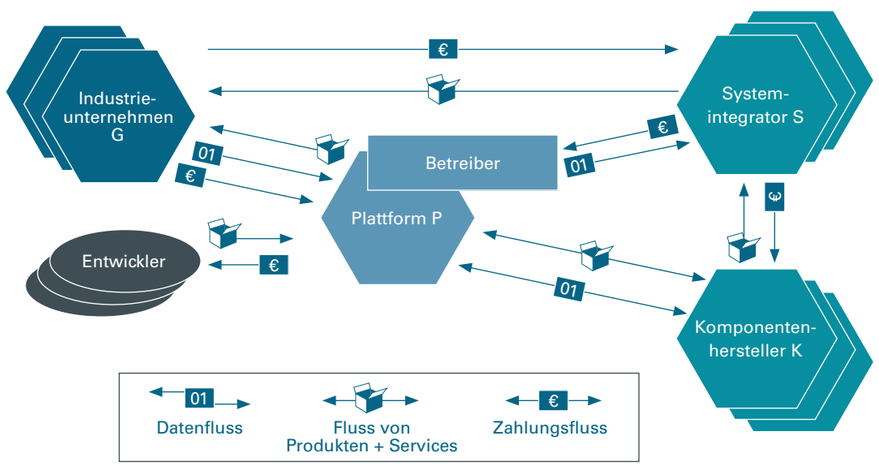
Dazu gehören insbesondere die Bereitstellung einer Entwicklungsumgebung sowie die Auswertung von Daten einzelner Komponenten der Anlagen. Darüber hinaus können weitere Dienstleistungsunternehmen, beispielsweise aus den Bereichen Mechanik, Elektronik oder Automation, über die Plattform eingebunden werden.

Die Beziehungen zwischen den Beteiligten stellen sich dabei wie folgt dar: Unternehmen aus dem produzierenden Gewerbe (anlagenbetreibende Unternehmen) geben Daten – in Form spezifischer Anforderungen an eine neu zu erstellende Produktionsanlage – an die Plattform weiter und finden dort geeignete Entwicklungsunternehmen, wofür sie eine Vergütung entrichten. Anlagenentwickelnde Unternehmen erhalten über die Plattform Zugang zu den eingestellten Daten und nutzen die Entwicklungsumgebung der Plattform für die Entwicklung der spezifischen Anlage. Im Anschluss beziehen sie die benötigten Komponenten von spezialisierten Herstellerunternehmen – deren genaue Spezifikationen für sie auf der Plattform einsehbar sind – und liefern die fertige Anlage an die jeweiligen anlagenbetreibenden Unternehmen. Die Produktlieferungen werden jeweils von entgegengesetzt gerichteten Zahlungsflüssen begleitet. Für die Auftragsvermittlung zahlen die anlagenentwickelnden Unternehmen ebenso eine Vergütung an die Plattform wie für die Nutzung der Entwicklungsumgebung.

Während des späteren Betriebs der Anlage werden von der Plattform verschiedene Daten der einzelnen Komponenten gesammelt und ausgewertet. Darauf aufbauend lässt sich beispielsweise ein datenbasiertes Beratungsangebot realisieren. Langfristig kann die Plattform z. B. auch die Vermittlung für Produktionskapazitäten der anlagenbetreibenden Unternehmen übernehmen. Ob die einzelnen Zahlungsströme an die Plattform als Einmalzahlungen, Abonnements oder anderweitig ausgestaltet werden, oder ob bestimmte Akteursgruppen die Plattform ggf. kostenlos nutzen können, richet sich nach dem individuellen Geschäftsmodell des plattformbetreibenden Unternehmens.

Robotik

Wertschöpfungssystem des Fallbeispiels Robotik

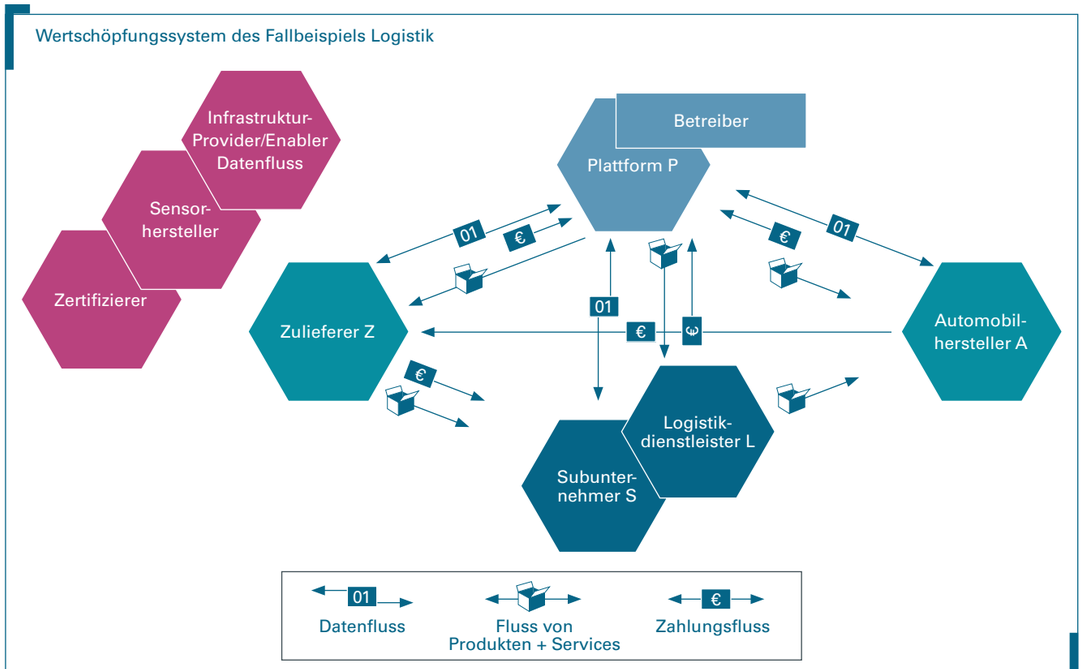


Im Mittelpunkt des hier dargestellten Robotik-Wertschöpfungssystems steht eine Plattform, die insbesondere kleinen und mittleren Unternehmen (KMU) als Anlaufstelle bei der Informationssuche und Planung von Robotik-Lösungen dient. Automatisierungslösungen im industriellen Umfeld werden in der Regel durch Systemintegratoren entwickelt und bereitgestellt. Ein nicht unerheblicher Teil der gesamten Kosten entfällt auf diese Dienstleistung. Für KMU sind Automatisierungslösungen damit häufig nicht abbildbar. Andererseits sind die kleinteiligen Aufträge auch für Systemintegratoren wenig lukrativ, da diese bei den KMU zunächst viel Aufklärungsarbeit zu den Automatisierungsmöglichkeiten leisten müssen. Die hier dargestellte Robotik-Plattform nimmt den Systemintegratoren daher einen Teil dieser Last ab und bietet KMU im Ergebnis eine günstigere Automatisierungslösung an. Den Herstellern von Robotikkomponenten und Standardlösungen bietet die Plattform zudem einen zusätzlichen Vertriebskanal und damit die Möglichkeit, zusätzliche Kundengruppen zu erreichen.

Die KMU melden dabei ihre spezifischen Anforderungen auf der Plattform an und bekommen erste Informationen darüber, welche ihrer Tätigkeiten prinzipiell automatisierbar sind. Über die Plattform werden den KMU dann geeignete Anbieterunternehmen für die Systemintegration vermittelt. Darüber hinaus bietet die Plattform den KMU Informationen zu verschiedenen Robotik-Komponenten und Standardlösungen. KMU können sich damit auf der Plattform eine Automatisierungslösung vorkonfigurieren und diese im Rahmen einer Simulation testen. Diese Dienstleistung nehmen die KMU entgeltlich in Anspruch (pauschal oder auch erst im Fall eines Auftrags an einen Systemintegrator). Die Systemintegratoren bekommen die Daten der vorkonfigurierten Lösung und setzen diese bei den KMU um, wofür sie von diesen eine entsprechende Vergütung erhalten. Die Komponenten der Automatisierungslösung beziehen die Systemintegratoren dabei entweder direkt von den Herstellerunternehmen oder auch über die Plattform. Die Produktlieferungen sind an jeweils entgegengesetzte Zahlungsströme gekoppelt. Zusätzlich lassen sich externe Entwicklerinnen und Entwickler sowie Dienstleistungsunternehmen über die Plattform integrieren.

Für einen schnellen Markteintritt bietet sich für die Plattform die Möglichkeit, existierende Standardlösungen („Stand-alone“ Geräte) anzubieten, welche ggf. softwareseitig angepasst werden. Langfristig wäre es darüber hinaus denkbar, dass die Plattform die Komponenten direkt über die Hersteller bezieht, um aufgrund hoher Abnahmemengen niedrigere Einkaufspreise zu erzielen. Systemintegratoren könnten dann die Komponenten über die Plattform beziehen und so von den günstigeren Konditionen profitieren.

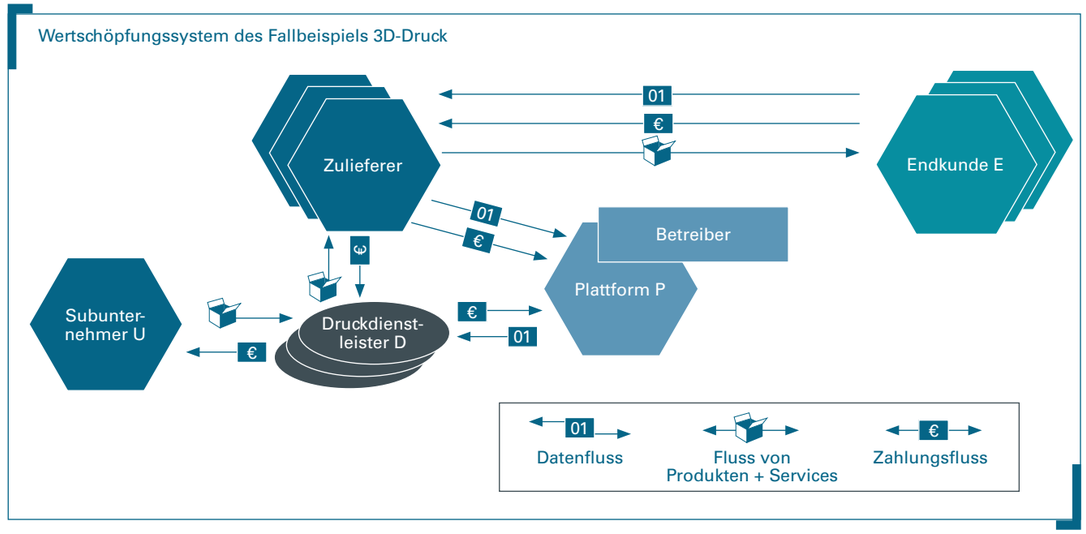
Logistik



Die hier dargestellte Logistik-Plattform bietet sowohl Herstellerunternehmen (z. B. aus dem Automobilbau) als auch deren Zuliefer- und Logistik-Dienstleistungsunternehmen die Möglichkeit, jederzeit aktuelle Informationen über den Zustand ihrer Ladungsträger zu erhalten und ihre eigenen Logistikprozesse zu optimieren. Zusätzlich kann die Plattform im Schadensfall als Clearingstelle agieren.

Die Plattform stellt den beteiligten Logistik-Dienstleistern intelligente Ladungsträger zur Verfügung. Diese verfügen über eine umfangreiche integrierte Sensorik, die permanent verschiedenste Umweltdaten aufzeichnet. Dazu gehören beispielsweise der Aufenthaltsort des Ladungsträgers, Temperatur im Ladungsträger, dessen Ladungszustand (leer oder befüllt) oder auch mögliche Defekte. Die Daten der Ladungsträger stellt das Unternehmen den Zulieferern und Herstellern zur Verfügung, wofür diese ein Entgelt entrichten. Darüber hinaus analysiert das plattformbetreibende Unternehmen diese Daten und stellt allen Beteiligten darauf aufbauende Dienstleistungen zur Verfügung. Dazu gehört beispielsweise die Optimierung der Fahrten der Logistik-Dienstleister sowie die Optimierung des Logistikprozesses der Zulieferer und Hersteller. Für diese Dienstleistungen zahlen die Unternehmen ebenfalls ein Entgelt. Als mögliche assoziierte bzw. kooperierende Akteursgruppen kommen in diesem Wertschöpfungssystem beispielsweise akkreditierte Zertifizierungs-Dienstleister, Hersteller von Sensoren sowie Infrastruktur-Provider in Betracht.

3D-Druck



Die hier abgebildete Plattform bietet ihrer Klientel einen schnellen transparenten Überblick über den Markt für 3D-Druck-Dienstleistungen. Dazu gehören insbesondere Informationen zu den relevanten Druckdienstleistungsunternehmen, deren vorhandene Druckmaschinen sowie ggf. Fertigungskapazitäten.

Die Plattform richtet sich dabei vor allem an Zulieferer, die ihrer Kundschaft individuell gedruckte Bauteile bereitstellen. Die Plattform nimmt dabei die spezifischen Daten der zu druckenden Bauteile auf und vermittelt geeignete Druckdienstleister. Von letzteren erhält die Plattform dabei Daten über die vorhandenen Druckmaschinen, deren Auslastung, die verfügbaren Produktionskapazitäten sowie nach erfolgter Beauftragung über den Stand des Drucks. Die Dienstleister geben die Aufträge je nach Auslastungsgrad und verfügbaren Maschinen ggf. an Subunternehmen weiter. Für die Zulieferer als Druckauftraggebende besteht die Möglichkeit, Druck- und Entwurfsdateien auf der Plattform zu hinterlegen und zu bearbeiten. Dafür erhält das plattformbetreibende Unternehmen ein Entgelt. Die Druckdienstleister zahlen darüber hinaus eine Vergütung für die vermittelten Aufträge. Die Lieferung der gedruckten Bauteile und deren Bezahlung erfolgen direkt zwischen Zulieferer und Druckdienstleister.

Eine Abwandlung des Wertschöpfungssystems besteht darin, dass die Plattform nicht der Vermittlung dient, sondern im eigenen Namen Druckdienstleistungen anbietet. Die Druckdienstleister fungieren in diesem Fall als Subunternehmen der Plattform. Waren- und Zahlungsströme verlaufen in diesem Fall direkt zwischen Plattform und Auftraggebenden.

2 Geschäftsmodelle entwickeln

2.1 Ein iterativer Prozess

Während der Geschäftsmodellentwicklung und -umsetzung wechseln sich unterschiedliche Aufgaben ab, die ggf. mehrmals bearbeitet werden müssen. Für ein besseres Verständis sowie zur Strukturierung des Vorgehens ist es sinnvoll, diesen Prozess in einzelne Schritte oder Phasen zu unterteilen. Der vorliegende Leitfaden orientiert sich an dem in Buchholz und Bürger (2020)[1] beschriebenen Vorgehensmodell. Die jeweiligen Phasen werden dabei nicht linear nacheinander durchschritten, sondern folgen einem iterativen Prozess. Grundsätzlich lässt sich dabei mit verschiedenen Phasen starten. Es können Phasen übersprungen oder auch wiederholt werden. Welches Vorgehen das richtige ist, richtet sich ganz nach den Bedarfen des jeweiligen Projekts. Im Folgenden werden die Phasen der Geschäftsmodellentwicklung und -umsetzung in einer Art idealtypischen Verlauf kurz beschrieben.

1. Bevor konkrete Ideen für neue Geschäftsmodelle entwickelt werden, sollte das Ökosystem analysiert werden, in welchem das neue Geschäftsmodell eingebettet sein wird. Dabei müssen die eigenen, internen Stärken und Schwächen sowie externe Chancen und Risiken berücksichtigt werden. Neben der klassischen SWOT-Analyse sollten dabei auch Tools eingesetzt werden, die es ermöglichen, die relevanten Anspruchsgruppen und Beteiligten sowie deren Motivation zu identifizieren und zu verstehen. Vor allem die Wünsche und Probleme der direkten Kundinnen und Kunden müssen erkannt werden, um ein Leistungsangebot erstellen zu können, welches deren Bedürfnisse gezielt adressiert. Dabei hat sich insbesondere das Kundenprofil aus dem Value Proposition Canvas[2] als nützliches Tool erwiesen. Das Canvas ist als Ergänzung des Business Model Canvas[3] anzusehen und zielt speziell auf die Entwicklung eines an den Bedürfnissen und Problemen von Kundinnen und Kunden ausgerichteten Wertversprechens. Gerade bei der Entwicklung von Geschäftsmodellen, die auf digitalen Dienstleistungen beruhen, lässt sich das Rollenmodell nach Papert (2018)[4] nutzen, um alle relevanten Akteursgruppen zu identifizieren. Mit der GEMINI[5] Modellierungssprache für Wertschöpfungssysteme lassen sich zudem die Beziehungen zwischen diesen Akteursgruppen anschaulich darstellen. Eine Besonderheit kollaborativer Geschäftsmodelle ist die Zusammenarbeit unterschiedlicher Akteursgruppen wie Hersteller, Zulieferer und Dienstleister. Daher empfiehlt es sich, bereits in dieser frühen Phase eine gemeinsame Vision für das Projekt zu entwickeln, damit alle Beteiligten auf das gleiche Ziel hinarbeiten. Dabei haben sich Workshops rund um das Thema „Storytelling“ als zielführend erwiesen. Nutzen lassen sich dabei z. B. Methoden wie der Golden Circle[6] oder die Heldenreise[7].

2. Den nächsten Schritt bildet die Ideenfindung. Dabei werden mit Hilfe von Kreativtechniken unterschiedliche Geschäftsmodellideen entwickelt. Ziel ist es, neuartige Wertangebote zu kreieren, die spezifisch auf die Bedürfnisse und Probleme von Kundinnen und Kunden eingehen. Dabei sollte über den eigenen Tellerrand geblickt werden. Geschäftsmodelle von Firmen aus anderen Branchen können entscheidende Denkanstöße geben. Bewußt eingesetzt wird dies beispielsweise bei der Arbeit mit den Karten zur Entwicklung von Geschäftsmodellen des St. Galler Business Model Navigator[8] oder dem GEMINI Geschäftsmodellmuster-Kartenset. Der St. Galler Business Model Navigator fasst dabei 55 erfolgreiche Geschäftsmodellmuster in einem Satz von Musterkarten zusammen. Jede dieser Karten enthält die wichtigsten Informationen, um das jeweilige Geschäftsmodellmuster zu erfassen und zu verstehen sowie konkrete Beispiele von Unternehmen, die dieses Geschäftsmodellmuster erfolgreich implementiert haben. Das GEMINI Kartenset stellt eine konsolidierte Version der St. Galler Geschäftsmodellmusterkarten dar, wobei ähnliche Geschäftsmodelle zusammengefasst und zusätzliche Geschäftsmodelle aus dem Kontext Industrie 4.0 ergänzt wurden. Das GEMINI Kartenset umfasst insgesamt 74 Geschäftsmodellmuster. Alternativ lassen sich aber auch allgemeine Kreativtechniken[9] nutzen.

3. Die einmal generierten Ideen müssen danach in einem weiteren Schritt bewertet und zu echten Geschäftsmodellen ausgestaltet werden. Nur so lässt sich eine Entscheidung darüber treffen, welche Geschäftsmodellidee für die spätere Umsetzung in Frage kommt. Hierbei kann auf eine Vielzahl verschiedenster Tools und Methoden zurückgegriffen werden wie das Value Proposition Canvas, das Business Model Canvas, das Magische Dreieck aus dem St. Galler Business Model Navigator[10] oder die GEMINI Modellierungssprache[11] für Wertschöpfungssysteme. In dieser Phase empfiehlt es sich, bereits die rechtlichen Rahmenbedingungen einzubeziehen, die für die Umsetzung des jeweiligen Geschäftsmodells relevant sind.

4. Neben der Ausgestaltung der einzelnen Geschäftsmodellideen müssen die ihnen zugrundeliegenden Annahmen überprüft werden. Als Datengrundlage können u. a. die amtlichen Statistiken des Bundes und der Länder dienen. Für spezifischere Informationen sollten eigene Daten erhoben werden. Dafür bieten sich z. B. Umfragen, Interviews oder Workshops mit der jeweiligen Zielgruppe und anderen Beteiligten des Geschäftsmodells an. Insbesondere Messebesuche oder -auftritte sind gut zur Befragung der Zielgruppe geeignet. Darüber hinaus lassen sich aber auch weitere Instrumente nutzen. Beispielsweise bietet eine Crowdfunding Kampagne eine gute Möglichkeit, die Präferenzen der Zielgruppe hinsichtlich Preis oder Produktvarianten zu testen.

5. Bevor ein Geschäftsmodell tatsächlich umgesetzt wird, ist es häufig sinnvoll, eine Prototyping-Phase zu durchlaufen. Prototypen dienen einerseits der Beurteilung der technischen Machbarkeit eines Produkts, andererseits können Sie für Akzeptanzprüfungen mit potenziellen Kundinnen und Kunden und anderen Anspruchsgruppen genutzt werden. Dabei gibt es sehr unterschiedliche Arten von Prototypen. Diese reichen vom einfachen Entwurfsmuster in der Softwareentwicklung bis hin zum funktionstüchtigen Vorab-Exemplar einer Serienfertigung. Reine Visualisierungen gehören ebenso dazu wie beispielsweise Clickdummies und miniaturisierte Modelle oder auch physische Prototypen in Originalgröße mit limitiertem Funktionsumfang.

6. Die letzte Phase der Geschäftsmodellentwicklung bildet die eigentliche Umsetzung und damit die Markteinführung. Zur Planung und Kontrolle von Experimenten lässt

1 Buchholz/Bürger (2020). Der Geschäftsmodell-Toolguide – Von der Idee zur Umsetzung, Campus Verlag, Frankfurt, New York.
2 https://www.strategyzer.com/blog/value-proposition-canvas-a-tool-to-understand-what-customers-really-want [14.07.2020]
3 https://www.strategyzer.com/canvas/business-model-canvas [14.07.2020]
4 Papert (2018): Entwicklung eines Ökosystemmodells für das Internet der Dinge, Fraunhofer Verlag.
5 https://www.geschaeftsmodelle-i40.de/fileadmin/Innowissen/GEMINI/GEMINI_Studie_Gesamt.pdf [14.07.2020]
6 Sinek (2014). Frag immer erst: warum: Wie Top-Firmen und Führungskräfte zum Erfolg inspirieren; Redline Verlag, Münchner Verlagsgruppe GmbH, München.
7 Campbell (2011). Der Heros in tausend Gestalten, Insel Verlag, Berlin.
8 https://bmilab.com [14.07.2020]
9 Vgl. Boysen (2020) Kreativitätsmethoden, in: Buchholz und Bürger (Hrsg.) Der Geschäftsmodell-Toolguide - Von der Idee zur Umsetzung, Campus, Frankfurt, New York.
10 https://bmilab.com [14.07.2020]
11 https://www.geschaeftsmodelle-i40.de/fileadmin/Innowissen/GEMINI/GEMINI_Studie_Gesamt.pdf [14.07.2020]

sich dabei zum Beispiel das Lean Dashboard Canvas[12] sinnvoll einsetzen. Allgemein spielen in dieser Phase jedoch Canvas-Tools eine eher untergeordnete Rolle. Bei der Umsetzung werden dagegen typischerweise Kennzahlen – sogenannte Key Performance Indicators oder KPIs – zur Erfolgskontrolle verwendet. Mit deren Hilfe lassen sich Fortschritt und Erfolg der Markteinführung messen und bewerten. Um frühzeitig planen zu können, wie das Geschäftsmodell sukzessive weiterentwickelt werden kann, lässt sich zudem eine Umsetzungsroadmap (z. B. Peitz, 2015)[13] nutzen. Für die Optimierung des Kundenerlebnisses nach der Markteinführung, bietet das Customer Journey Design[14] Orientierung. Darüber hinaus existieren spezialisierte Tools und Methoden, wie z. B. der Ordnungsrahmen Smart-Service-Vertrieb[15], der bei der Markteinführung digitaler Produkte ganzheitlich unterstützt.

2.2 Wertschöpfungssysteme darstellen

Durch eine grafische Darstellung von Wertschöpfungssystemen lassen sich kollaborative Geschäftsmodelle modellieren. Prinzipiell umfasst diese Darstellung alle an der Leistungserstellung beteiligten Organisationseinheiten und Prozesse. Dazu gehören neben organisationsspezifischen Arbeitsabläufen auch unternehmensübergreifende Wertschöpfungsaktivitäten.[16]

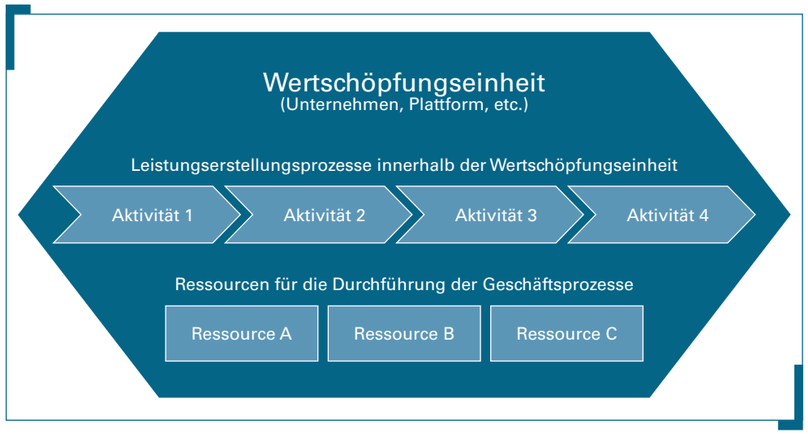
Die Modellierung des Wertschöpfungssystems dient dabei zunächst einmal der Veranschaulichung aller Wertschöpfungsaktivitäten und hilft, bei den Beteiligten ein gemeinsames Verständnis aller Prozesse zu etablieren. Insbesondere bei der Entwicklung kollaborativer Geschäftsmodelle mit verschiedenen Partnerorganisationen und teils sehr unterschiedlichen Interessenslagen ist es wichtig, eine gemeinsame Vorstellung des zukünftigen Wertschöpfungssystems zu entwickeln. Alle Beteiligten sollten sich darin wiederfinden und die eigene Rolle entsprechend berücksichtigt wissen. Darüber hinaus ermöglicht die Visualisierung, auch juristische Fallbeispiele abzuleiten, die der Klärung rechtlicher Fragestellungen dienen.

Das Ausarbeiten relevanter rechtlicher Fragestellungen sollte dementsprechend bereits bei der Bewertung und Ausgestaltung der Geschäftsmodellideen erfolgen. Einerseits ist es ratsam die rechtlichen Aspekte bereits in die Bewertung der einzelnen Geschäftsmodellideen einfließen zu lassen, um keine Geschäftsmodelle zu verfolgen, welche später erhebliche juristische Risiken bergen. Andererseits müssen die Geschäftsmodelle hinreichend genau beschrieben und ausgestaltet sein, um rechtliche Fragestellungen überhaupt ableiten und beantworten zu können. Insbesondere die unternehmensübergreifenden Wertschöpfungsaktivitäten, das Partner- und Lieferantennetzwerk sowie die Austauschbeziehungen mit Partnerorganisationen und Kundinnen und Kunden sind dafür relevant.

Zur Modellierung und Darstellung der Wertschöpfungssysteme hat sich z. B. die GEMINI Modellierungssprache als nützliches Tool erwiesen. Sowohl in verschiedenen Workshops als auch bei der Erstellung der in Kapitel 1.1 vorgestellten Wertschöpfungssysteme wurden mit der Methotik gute Erfahrungen gemacht – wobei einige kleinere Anpassungen hinsichtlich der spezifischen Anforderungen unterschiedlicher Rollen und Beziehungen zwischen den Beteiligten von kollaborativen Wertschöpfungssystemen vorgenommen wurden.

12 https://leanstack.com [14.07.2020]
13 Peitz (2015): Systematik zur Entwicklung einer produktlebenszyklusorientierten Geschäftsmodell-Roadmap, Paderborn: HNI-Verlagsschriftenreihe, Band 337.
14 Vgl. Frank, J.; Leiting, T. (2020) Customer Journey Design, in: Der Geschäftsmodell-Toolguide, Campus, Frankfurt, New York.
15 Vgl. Frank, J.; Faulhaber, M. (2020) Ordnungsrahmen Smart-Service-Vertrieb, in: Der Geschäftsmodell-Toolguide, Campus, Frankfurt, New York.
16 Gausemeier/Wieseke/Echterhoff/Koldewey/Mittag/Schneider/Isenberg (2017): Mit Industrie 4.0 zum Unternehmenserfolg - Integrative Planung von Geschäftsmodellen und Wertschöpfungssystemen, Paderborn: Heinz Nixdorf Institut.

Die Modellierungssprache setzt prinzipiell auf den Informationen aus dem Business Model Canvas auf. Im Mittelpunkt des Wertschöpfungssystems steht dabei die zu betrachtende Wertschöpfungseinheit (Unternehmen, Abteilung, Plattform etc.). Diese wird im Zentrum des Wertschöpfungssystems als Hexagon dargestellt. Die Schlüsselaktivitäten aus dem Business Model Canvas bilden die relevanten Leistungserstellungsprozesse ab. Diese werden als aufeinanderfolgende Wertschöpfungsaktivitäten innerhalb der Wertschöpfungseinheit dargestellt. Die Schlüsselressourcen aus dem Business Model Canvas werden ebenfalls in die zu betrachtende Wertschöpfungseinheit integriert.



Darüber hinaus müssen alle weiteren relevanten Akteursgruppen identifiziert werden. Diese werden im Anschluß um die zu betrachtende Wertschöpfungseinheit gruppiert, so dass die Beziehungen zwischen allen Beteiligten des Wertschöpfungssystems dargestellt werden können.

Nachdem die Wertschöpfungsprozesse innerhalb der zu betrachtenden Wertschöpfungseinheit abgebildet wurden, müssen die Beziehungen zwischen den Beteiligten des Geschäftsmodells dargestellt werden. Diese bilden dabei die Knoten eines Netzwerkes. Daher ist es notwendig, alle aktiv Beteiligten zu spezifizieren. Beteiligte können sowohl Personen als auch Unternehmen, Verbände, Organe der öffentlichen Verwaltung und andere Organisationen bzw. Organisationseinheiten sein. Um nicht jeden Beteiligten einzeln aufführen zu müssen, bietet es sich in der Regel an, diese zu Gruppen zusammenzufassen. Allerdings ist es durchaus möglich, dass wichtige Schlüsselkooperationen oder bei hochspezialisierten Angeboten einzelne Schlüsselkundinnen und -kunden separat dargestellt werden.

Bei der kollaborativen Entwicklung von (insbesondere plattformbasierten) Geschäftsmodellen stellt sich häufig die Frage nach dem Betriebskonzept. Ein gemeinschaftlich entwickeltes Geschäftsmodell kann sowohl individuell durch ein einzelnes Unternehmen als auch kollektiv durch ein Konsortium von Unternehmen, einem Verein oder einem Verband betrieben werden. Daher gilt es dringend zu klären, wer als betreibende Organisation der Wertschöpfungseinheit agiert.

Neben dem betreibenden Unternehmen bilden die Kundinnen und Kunden die vielleicht wichtigste Gruppe des Wertschöpfungssystems. Während bei der detaillierten Analyse der Kundengruppen (z. B. mit dem Value Proposition Canvas) unbedingt zwischen Anwendenden und Kaufenden unterschieden werden sollte, kann darauf bei der Darstellung des Wertschöpfungssystems zugunsten der Übersichtlichkeit in der Regel verzichtet werden.

Eine weitere Gruppe von Beteiligten bilden die relevanten Schlüsselkooperationen der Wertschöpfungseinheit. Dazu gehören beispielsweise Kooperationen im Vertrieb, in der Produktion oder in der Entwicklung sowie mit anderen spezialisierten Dienstleistern. Die Unterscheidung zwischen Partnerschaften und Kundinnen und Kunden kann teilweise weniger offensichtlich sein als erwartet. So zählen Anbietende, die ihre Produkte und Dienstleistungen über eine Plattform an ihre Kundinnen und Kunden vertreiben, für die Plattform ebenso zu den Partnerschaften als auch zu den Kundinnen oder Kunden. Für die Darstellung des Wertschöpfungssystems spielt diese Unterscheidung jedoch zumeist eine untergeordnete Rolle.

Nachdem alle relevanten Beteiligten abgebildet sind, gilt es, die Beziehungen zwischen diesen darzustellen. Zu den Beziehungen zählen Kommunikationsbeziehungen, der Austausch von Produkten und Dienstleistungen, Zahlungsflüsse und Datenströme.

Der Austausch von Produkten und Dienstleistungen geht häufig mit entgegengesetzten Zahlungsflüssen einher, d. h. Kundinnen und Kunden zahlen für die gelieferten Leistungen. Allerdings sind Kundinnen und Kunden nicht notwendigerweise auch diejenigen, die für die Produkte und Dienstleistungen zahlen. Dies ist insbesondere dann der Fall, wenn Produkte und Dienstleistungen kostenlos zur Verfügung gestellt und beispielsweise durch Werbeeinnahmen finanziert werden.

Gerade bei datenbasierten Geschäftsmodellen ist es vor allem im Hinblick auf die Beantwortung rechtlicher Fragestellungen wichtig, darzustellen, zwischen welchen Beteiligten Daten ausgetauscht werden sollen. Dies wird besonders offensichtlich, wenn Dienstleistende Zugriff auf sensible Unternehmensdaten von Kundinnen und Kunden erhalten sollen. Aber auch für die Einhaltung der Bestimmungen der europäischen Datenschutz-Grundverordnung (zur DSGVO s. Kapitel 3.3.1) ist es elementar, sich zu vergegenwärtigen, welche Daten zwischen welchen Beteiligten ausgetauscht werden sollen.

2.3 Herausforderungen bei der Entwicklung kollaborativer Geschäftsmodelle

2.3.1 Ein gemeinsames Verständnis entwickeln

Die Entwicklung von kooperativen Geschäftsmodellen stellt die Beteiligten vor technische, wirtschaftliche, organisatorische und rechtliche Herausforderungen. Von einer systematischen Entwicklung und Implementierung, die frühzeitig unterschiedliche Interessenslagen und eine faire Risiko- und Chancenverteilung berücksichtigt, profitieren alle Beteiligten. Die unterschiedlichen technischen, wirtschaftlichen, rechtlichen und organisatorischen Anforderungen der Beteiligten zusammenzuführen, stellt gleichzeitig eine der größten Herausforderungen bei der Entwicklung kollaborativer Geschäftsmodelle dar.

Da es bisher kaum erfolgreiche Beispiele kollaborativer Geschäftsmodelle gibt, ist die konkrete Ausgestaltung dieser Wertschöpfungssysteme mit sehr großen Unsicherheiten verbunden. Ausschlaggebend für den Erfolg ist die gemeinschaftliche Klärung der Interessen, der Motivation und des Nutzens für alle Beteiligten. Häufig wird diese Aufgabe unterschätzt und ein Geschäftsmodell beispielsweise nur auf das plattformbetreibende Unternehmen hin optimiert. Wenn jedoch nicht für alle Seiten hinreichend Mehrwert generiert wird, bleibt der Erfolg der gemeinsamen Lösung aus.

Zu empfehlen ist, mit allen Beteiligten (z. B. Entwicklerinnen und Entwickler, Technologieunternehmen, Zulieferunternehmen etc.) – auch unter Einbindung von Kundinnen und Kunden – in moderierten Geschäftsmodell-Workshops die unterschiedlichen Vorstellungen, Bedürfnisse und Interessenslagen frühzeitig zu diskutieren. Was ist die gemeinsame Vision für das Geschäftsmodell? Welche Leistungen sollen etwa über eine Plattform für welche Zielgruppen angeboten werden? Welchen Mehrwert bietet das kollaborative Geschäftsmodell sowohl für die einzelnen Konsortialbeteiligten als auch für die unterschiedlichen Klientelgruppen? Welche Rollen übernehmen die einzelnen Beteiligten? Diese und weitere Fragen sollten in Geschäftsmodell-Workshops diskutiert werden. Dabei ist das Ziel, ein gemeinsames Verständnis für das Zusammenspiel der verschiedenen Beteiligten und des kollaborativen Geschäftsmodells bzw. der Plattform zu entwickeln.

Um ein gemeinsames Verständnis für das Ökosystem einer zu entwickelnden Plattform zu schaffen und herauszuarbeiten, welchen Mehrwert die Plattform allen Beteiligten sowie den unterschiedlichen Klientelgruppen bieten kann, hat sich die Anwendung des Platform Value Canvas aus dem Platform Innovation KIT[17] bewährt. Nach der Definition aller Plattform-Beteiligten werden zunächst die Vorteile für jede Anspruchsgruppe erarbeitet. Es geht bei diesem Schritt nicht um die Beschreibung der Leistung, sondern der Vorteile (Benefits) für alle Beteiligten (z. B. zusätzliche Umsätze, neue Vertriebskanäle, Vernetzung, Kosteneinsparungen). Im Workshop sollte diskutiert werden, ob das kooperative Geschäftsmodell bzw. die Plattform tatsächlich ausreichende Mehrwerte bietet und diese auch zu den Bedürfnissen der unterschiedlichen Anspruchsgruppen passen. Sind sich dann alle Beteiligten einig, können in einem nächsten Schritt die Transaktionen (Informations- und Werteflüsse) und die Monetarisierungsstrategien als Geldflüsse zwischen den Beteiligten herausgearbeitet werden.

2.3.2 Das Betriebsmodell erarbeiten

Von zentraler Bedeutung bei kollaborativen Geschäftsmodellen ist das Betriebsmodell. Bei einer Plattform ist beispielweise das plattformbetreibende Unternehmen für die Entwicklung, Umsetzung und Aufrechterhaltung der Plattform verantwortlich. Es kontrolliert und verwaltet die Infrastruktur und die Kernkomponenten, die das Funktionieren der Plattform und die Nutzung und Anbindung aller Beteiligten und Anwendenden sicherstellen. Dazu können neben technischen Applikationen auch Standards gehören, auf die sich die Beteiligten geeinigt haben. Zudem ist das betreibende Unternehmen auch für die Einhaltung der rechtlichen Rahmenbedingungen, insbesondere zur IT-Sicherheit und zum Datenschutz sowie für den Aufbau einer gesetzeskonformen IT-Infrastruktur verantwortlich. Auf die relevanten rechtlichen Aspekte wird in Kapitel 3 im Detail eingegangen.

Die Rolle des plattformbetreibenden Unternehmens kann individuell von einem bestehenden Unternehmen (z. B. bei einer zentralen Plattform) oder auch gemeinschaftlich von den Kooperierenden übernommen werden – beispielsweise in Form einer Betriebsgesellschaft oder durch die Gründung eines Vereins oder eines Verbandes. In diesem Zusammenhang ist es auch wichtig, frühzeitig die Risikoverteilung bei der Finanzierung, bei der Produkt-

17 https://platforminnovationkit.com/ [14.07.2020]

haftung und beim Datenschutz zu diskutieren. Beispielsweise ist für eine neu gegründete Betriebsgesellschaft eine Finanzierung der Entwicklung, Umsetzung und Markteinführung durch die Aufnahme von Risikokapital einfacher umzusetzen. Bei der Produkthaftung ist es entscheidend, ob eine Plattform lediglich in einer Vermittlungsfunktion agiert oder Leistungen und Produkte im eigenen Namen anbietet. Ein plattformbetreibendes Unternehmen, das nur die Vermittlung übernimmt, haftet beispielsweise nicht für die Leistungen der in die Plattform eingebundenen Unternehmen, die im eigenen Namen aktiv sind (s. zu Haftungsfragen im Detail Kapitel 3.2).

Die Wahl eines geeigneten Betriebsmodells ist jedoch auch abhängig von Sinn und Zweck des kollaborativen Wertschöpfungsmodells. Beispielsweise sind dezentrale Plattformen insbesondere für die Umsetzung verteilter Wertschöpfung geeignet und funktionieren ohne zentrale Betreibende. Hierfür bietet die Nutzung von Distributed-Ledger-Technologien (DLT) – z. B. einer Blockchain – als dezentrale und vertrauensbildende Technologie transparente und sichere Transaktionen. Da der Schutz vor Datenmanipulation, die Verifizierbarkeit und Nichtveränderlichkeit von Daten in dieser Technologie und deren Architektur verankert sind, ist das Potenzial von DLT für die Umsetzung von dezentralen Plattformen für verteilte Wortschöpfung groß. Hochsensible Daten zu verfügbaren Kapazitäten, Maschinen- und Produktdaten, unternehmensinternen Planungsdaten sowie Informationen, wie Buchungen und Kaufverträge oder Transaktionen, wie Zahlungen oder die Einräumung von Nutzungsrechten, lassen sich durch die Blockchain-Technologie eindeutig verifizieren und direkt und sicher zwischen den verschiedenen Agierenden austauschen.[18]

2.3.3 Datenzugang und -nutzung

Daten werden für die Wertschöpfung immer bedeutender. Die Nutzung von Daten und deren Analyse ermöglicht es, neue Geschäftsmodelle umzusetzen und die Marktposition zu stärken. Bei der Umsetzung kollaborativer Geschäftsmodelle ist es wichtig, dass sich alle Beteiligten vertraglich darüber einigen, wer welche Daten zu welchem Zweck bereitstellt oder auswerten darf. Mit geeigneten technischen und organisatorischen Maßnahmen sollte überprüfbar sein bzw. gewährleistet werden können, dass sich die Beteiligten an die vertraglichen Vereinbarungen halten.

Beteiligte eines kollaborativen Geschäftsmodells sollten sich frühzeitig mit den rechtlichen Aspekten von datenbasierten Geschäftsmodellen auseinander setzen. Zu beachten ist dabei, dass es derzeit kein „Dateneigentumsrecht“ gibt. Daten gelten nicht als Sachen und können daher nicht Gegenstand einer Übereignung sein. Es können aber beispielsweise vertragliche Nutzungsberechtigungen an Daten eingeräumt werden. Dabei sollten die Befugnisse der Nutzungsberechtigten klar geregelt und auch Aspekte der risikogerechten Vertragsgestaltung berücksichtigt werden. Wichtig ist auch zu wissen, dass die Verarbeitung der Daten grundsätzlich nur mit Zweckbestimmung möglich ist und bei personenbezogenen Daten Art. 6 der DSGVO (Einwilligung, Vertragserfüllung) zu beachten ist, bei Daten von Mitarbeitenden darüber hinaus auch die Vorschriften des BDSG (§ 26). Werden auf einer kollaborativen Plattform durch die Beteiligten gemeinschaftlich Daten verarbeitet, besteht nach der DSGV (Art. 26) auch eine gemeinsame Verantwortlichkeit (Joint Controllership). Zwischen den Beteiligten müssen dann entsprechende Vereinbarungen geschlossen werden, auf die vertiefend in Kapitel 3 eingegangen wird.

18 Vgl. Buchholz/Wangler (2016): Neue Wege der Wortschöpfung und Kooperation, in Wittphal (Hrsg.) Digitalisierung iit Themeband Digitaisierung, S. 182.

3 Rechtlicher Rahmen für die Umsetzung kollaborativer Geschäftsmodelle

Viele der folgenden Überlegungen gelten für die meisten kollaborativen Geschäftsmodelle; eine wichtige Besonderheit stellt gerade die Interaktion über digitale Plattformen dar, auf die an verschiedenen Stellen hingewiesen wird. Wo zwischen den verschiedenen Gruppen besondere Unterschiede von Bedeutung sind, wird gesondert hingewiesen.

3.1 Vertragskonstellationen

3.1.1 Vertragliche Konstellationen und Vertragstypen

Den oben dargestellten Wertschöpfungsprozessen bzw. -einheiten und den einbezogenen Beteiligten sowie deren Beziehungen sind aus rechtlicher Sicht vertragliche Konstellationen zuzuordnen. Eine Zuordnung von Vertragskonstellationen oder -modellen ermöglicht zum einen die rechtliche „Verprobung“ der Idee. Sie gibt eine Antwort auf den „Rechtsreflex“ der Wertschöpfungsidee: Welche vertraglichen Gestaltungsmöglichkeiten erscheinen sinnvoll, weil sie den Interessen der Beteiligten oder zumindest einer/s Beteiligten weitestgehend Rechnung tragen? Welche Voraussetzungen wären zu schaffen, welche Risiken sind bereits zu erkennen und welche Akzeptanz fände das Modell wohl in seiner rechtlichen Ausgestaltung? Ebenso stellen sich Fragen nach Anpassungsfähigkeit des einmal definierten Modells und der Handhabbarkeit im Rahmen eines Vertragsmanagements. Diese frühe Befassung mit vertragsrechtlich naheliegenden Gestaltungsmöglichkeiten wirkt in der Regel auch zurück auf die Gestaltung des Wertschöpfungsmodells und erfüllt damit auch die Funktion eines Korrektivs.

Zum anderen ist die Zuordnung notwendige Voraussetzung für eine Vertragsgestaltung. Vor und während der Vertragsgestaltung ist zu prüfen, welche konkreten Leistungsverhältnisse zwischen welchen Parteien zustande kommen sollen. Jedes der in Kapitel 1 vorgestellten beispielhaften Wertschöpfungsmodelle besteht aus Leistungen unterschiedlicher Art. Rechtlich sind somit unterschiedliche Vertragstypen mit wiederum unterschiedlichen Rechtsfolgen (z. B. hinsichtlich der Haftung, siehe unten) einschlägig, die an vielerlei Stellen zu sogenannten typengemischten Verträgen führen. Zudem werden zur Umsetzung eines Wertschöpfungsmodelles diverse Verträge erforderlich werden, die zum Teil aufeinander abzustimmen sind, z. B. dort, wo ein Endkundenvertrag ein Leistungsversprechen lediglich in dem Umfang abgeben sollte, wie der Schuldner selbst Gläubiger gegenüber einem Zulieferunternehmen ist.

Soweit beispielsweise dem Kunden entgeltlich die Zusammenstellung einer Information (siehe Fallbeispiel Logistik) überlassen werden soll, kann hier eine Dienstleistung nach § 611 BGB, ein Werkvertrag nach § 631 BGB oder auch ein Vertrag mit Leistungsaspekten aus beiden Bereichen vorliegen. Ein Dienstvertrag würde in der Regel an die Tätigkeit des Zusammenstellens der Informationen anknüpfen und eine Vergütung nach Aufwand vorsehen. Gleiches gilt grundsätzlich für Beratungsleistungen. In einem Werkvertrag hingegen verspricht ein Unternehmer die Herstellung eines (abnahmefähigen) Werkes. Hier kommt es auf das Eintreten des vereinbarten Erfolgs an. Das Werkvertragsrecht kennt ein Mangelrecht in einer dem Kaufrecht ähnlichen Weise, § 633 ff. BGB. Der Dienstvertrag hingegen nicht.

Wird z. B. ein Vertrag zwischen einem Plattform-Betreiber und dem Plattform-Nutzer geschlossen, der im Wesentlichen die Nutzungsmöglichkeit der Online-Plattform mit den technisch zur Verfügung gestellten Funktionalitäten umfasst (ggf. Fallbeispiel Engineering), kann ein Nutzungsvertrag in Betracht kommen, der sich nach Mietrecht (analog) richtet. Gleiches gilt für Infrastructure as a Service (IaaS), Platform as a Service (PaaS) und Software as a Service (SaaS), die meist als typengemischte Verträge mit überwiegend mietvertraglichen Aspekten zu betrachten sind.[19] Im Fokus eines solchen Vertrages werden Verfügbarkeitsregelungen stehen, die klarstellen, welche technischen Erwartungen zu erfüllen sind, wie dies geprüft wird und welche Rechtsfolgen an das Unterschreiten der vereinbarten Parameter geknüpft sind.

Kollaborative Wertschöpfungsmodelle lassen in der Gestaltungsphase diverse Spielräume offen, den Beteiligten einzeln oder in Verbünden unterschiedliche rechtliche Rollen und Verantwortlichkeiten zuzuordnen. Vor der Erstellung von Verträgen sind diese Spielräume zu schließen. Es ist festzulegen, ob und inwieweit eine Leistung durch einen Beteiligten allein oder in einer Gesellschaft mit anderen Unternehmen erbracht bzw. gefordert werden soll.

3.1.2 Allgemeine Geschäftsbedingungen

Die Ausgestaltung eines Vertrags ist grundsätzlich den Parteien selbst überlassen. Es gibt jedoch gesetzliche Beschränkungen der Vertragsfreiheit. Neben den oben schon dargestellten Grenzen sind im deutschen Zivilrecht insbesondere die Einschränkungen mit Blick auf Allgemeine Geschäftsbedingungen (AGB) von Bedeutung. In §§ 305-310 BGB finden sich unter anderem Vorgaben zu Haftungsbeschränkungen oder Pauschalisierung von Schadensersatzansprüchen. Plattformbetreibende oder Hersteller möchten regelmäßig AGB in ihren Verträgen einsetzen, um bestimmte Fragen für alle künftigen Vertragspartner schon vorab zu regeln. Dafür müssen sie sich die Grenzen dieses Einsatzes bewusstmachen. Wenn etwa ein plattformbetreibendes Unternehmen in seinen AGB die Haftung für Schäden, die durch auf der Plattform angebotene Produkte entstehen, pauschal ausschließen will, muss es wissen, ob das zulässig ist. Die gesetzlichen Beschränkungen des AGB-Rechts sind relevant zwischen Unternehmen und Verbraucherinnen bzw. Verbrauchern, aber auch zwischen den Unternehmen. Sie gelten also etwa auch für die Verträge zwischen einer plattformbetreibenden Organisation und einem Unternehmen, das auf der Plattform Waren anbietet.[20] Diejenige Partei, die einen Vertrag entwirft, muss wissen, ob sie dabei eigentlich AGB einsetzt, ob diese wirksam Bestandteil des Vertags werden und ob sie im Einzelfall wirksam und zulässig sind.

Was AGB sind, legt § 305 BGB fest. Danach sind AGB „alle für eine Vielzahl von Verträgen vorformulierten Vertragsbedingungen, die eine Vertragspartei (Verwenderin) der anderen Vertragspartei bei Abschluss eines Vertrags stellt." Dabei kommt es nicht auf die Art und Weise der Ausgestaltung oder die äußere Form der Vertragsbedingungen an. Notwendig ist aber, dass die Vertragsbedingungen nicht „im Einzelnen ausgehandelt sind." Eine individuell ausgehandelte Vertragsbedingung stellt keine AGB vor. AGB sind nur dann Bestandteil eines Vertrags, wenn sie wirksam einbezogen werden. Hierzu muss die Vertragspartei auf die AGB hingewiesen werden und die Möglichkeit haben, von dieser Kenntnis zu nehmen. Auch wird festgelegt, dass wenn individuell zu einem speziellen Aspekt etwas anderes vereinbart

19 Vgl. BGH, Urteil vom 15.11.2006 – XII 120/04 (ASP-Entscheidung).
20 Vgl. § 310 Abs. 1 S. 2 BGB, außerdem Abschlussbericht des Forschungsprojekts „AGB-Recht für Verträge zwischen Unternehmen" (Leuschner/Meyer, 2014, http://www.bmjv.de/SharedDocs/Downloads/DE/Fachinformationen/Abschlussbericht-AGB-Forschungsprojekt.pdf?__blob=publicationFile) [14.07.2020]

wurde, diese Vereinbarung Vorrang hat – auch wenn die AGB insgesamt wirksam Bestandteil des Vertrags geworden sind.[21] Damit soll verhindert werden, dass vertragliche Vereinbarungen durch abweichende AGB ausgehöhlt oder zunichte gemacht werden.[22] Ebenso wenig werden überraschende Klauseln Bestandteil des Vertrags. Zweifel bei der Auslegung von AGB, etwa wenn eine Klausel mehrdeutig ist, gehen grundsätzlich zu Lasten der Verwenderin.[23] Unwirksame Regelungen im Rahmen von AGB haben aber nicht zur Folge, dass der Vertrag insgesamt unwirksam wird. Eine Ausnahme gilt nur dann, wenn der Fortbestand des Gesamtvertrags für eine Vertragspartei eine unzumutbare Härte darstellen würde.[24] Wenn im Hinblick auf die Auslegung von AGB Unklarheiten entstehen, wie etwa nun die Haftung aussehen soll, finden sich hierzu Antworten in den allgemeinen Gesetzen für bestimmte Vertragstypen (siehe Kapitel 4.1.1). Erweist sich beispielsweise eine Regelung zum Haftungsausschluss als unwirksam, so sind die gesetzlichen Haftungsregelungen anzuwenden, mit der Folge, dass bereits eine leichte Fahrlässigkeit zur Haftung führt.

Vermittlerplattformen machen oft inhaltliche Vorgaben für die Verträge zwischen ihren Nutzerinnen und Nutzern, etwa um so die Nutzung attraktiver oder sicherer zu machen. Eigentlich sind sie an den Verträgen zwischen diesen Parteien aber selbst nicht beteiligt. Im Ergebnis besteht zwischen Juristinnen und Juristen Einigkeit, dass diese Vorgaben der Plattform auch zwischen den Nutzerinnen und Nutzern gelten.[25]

Für die Vertragsgestaltung durch Plattformbetreibende oder Hersteller bedeutet das, dass sich AGB zweifellos grundsätzlich eignen, Vereinbarungen für eine größere Anzahl von Verträgen einzusetzen. Dabei muss aber gerade der Verwenderin bewusst sein, dass

- sie dafür Sorge trägt, dass sie zum Vertragsbestandteil werden und
- keine abweichende Individualabrede getroffen wird,
- sowohl Unwirksamkeit als auch Unklarheiten bei der Auslegung zu ihren Lasten gehen,
- sie sich innerhalb des vom Gesetz gegebenen Rahmens bewegen muss und
- ihrer Gestaltungsfreiheit damit Grenzen gesetzt sind.

Deshalb sollte bei ihrer Gestaltung der AGB eine auf den Einzelfall zugeschnittene Rechtsberatung erfolgen.

Alle Nutzerinnen und Nutzer der Plattformen (Anbieter und Kundinnen und Kunden) müssen überprüfen, ob

- durch die AGB des betreibenden Unternehmens inhaltliche Vorgaben für die Verträge zwischen ihnen vorliegen,
- sie diese wirksam individuell abändern können,
- ob und wie sie hierfür selbst AGB verwenden können.

21 § 305b BGB
22 MüKo BGB-Basedow, § 305b, Rn. 1.
23 § 305c BGB
24 § 306 BGB
25 Vgl. etwa BGH, NJW 2002, 363. Hierzu gibt es unterschiedliche Begründungen. Überzeugend ist wohl die Begründung, dass die Nutzerinnen und Nutzer schon mit der Erklärung, miteinander einen Vertrag eingehen zu wollen, automatisch auch gegenseitig die Erwartungen erfüllen wollen, die sich aus diesen AGB der Plattform ergeben.

3.2 Haftungsfragen und Risikomanagement

3.2.1 Was heißt Haftung? Welche Haftungsarten kommen in Betracht?

Nicht immer halten sich alle Beteiligten an alle Regeln. Gelegentlich werden, selbst wenn sich an alle Regeln gehalten wird, Unbeteiligte durch ein eigenes Verhalten oder ein Produkt geschädigt. In solchen Fällen kann es sein, dass ein oder mehrere Beteiligte haften. Denn die Einhaltung von Verträgen und Rechtsnormen wird unter anderem durch diese Haftung gesichert. Nur so können Betroffene für die von ihnen oft unverschuldete Schädigung einen Ausgleich erhalten.

Plattformbetreibende und Hersteller können in verschiedenster Weise riskieren, selbst oder zumindest als eine/r von mehreren Beteiligten oder als Unternehmen zu haften. Hiervor kann sich durch Vertragsgestaltung und Einhaltung der relevanten Vorgaben geschützt werden. Gelegentlich können sie auch von anderen Zahlungen fordern, wenn sie selbst geschädigt wurden.

Im Recht ist zwischen verschiedenen Möglichkeiten der Haftung zu unterscheiden, welche alle in ein präventives Risikomanagement der Plattformbetreibenden und Hersteller einzubeziehen sind.

Es gibt zivilrechtliche Haftung, die meist auf finanziellen Ausgleich gerichtet ist. Dazu gehören die vertragliche Haftung, die deliktische Haftung für Personen, zwischen denen keine vertraglichen Beziehungen bestehen, sowie die speziellen Formen der Produzentenhaftung und der davon zu unterscheidenden Produkthaftung. Alle kommen für Plattformbetreibende und Hersteller in Frage.

Daneben tritt das Strafrecht. Haftung nach diesem Rechtsgebiet bedeutet Bestrafung von einzelnen Handelnden, meist mittels Geldstrafe, ausnahmsweise auch Freiheitsstrafe (bei schweren oder wiederholten Straftaten). Das hat typischerweise keinen Ausgleich für das Opfer zur Folge[26] und trifft gerade die Täterin oder den Täter, ggf. auch mehrere Täterinnen und Täter. Wenn ein plattformbetreibendes Unternehmen an der Vermittlung eines Produkts mitwirkt, von dem es weiß, dass es nicht ordnungsgemäß zugelassen wurde, und hierdurch eine dritte Person geschädigt wird, kann es wegen fahrlässiger Körperverletzung strafbar sein. Auch hiergegen muss als plattformbetreibendes oder herstellendes Unternehmen Risikomanagement betrieben werden, indem alle relevanten Vorgaben eingehalten und sich sorgfaltsgemäß verhalten wird (siehe dazu unten, Ausführungen im Kapitel Risikomanagement).

3.2.2 Zivilrechtliche Haftung – Was ist das?

Zivilrechtliche Haftung bedeutet, dass eine Privatperson verpflichtet wird, gegenüber einer anderen Privatperson eine bestimmte Leistung zu erbringen. In der Regel geht es um finanziellen Ausgleich, typischerweise nach der Verletzung einer Pflicht (etwa aus Vertrag) oder eines Interesses einer anderen Person (z. B. Deliktsrecht). Verletzt also das Produkt eines Herstellers eine Kundin oder einen Kunden, kann es zivilrechtlich haften und muss gegebenenfalls Ausgleich für die Schäden der Kundin oder des Kunden bezahlen.

26 Bis auf gelegentlichen Täter-Opfer-Ausgleich.

3.2.3 Vertragliche Haftung

Welche Vertragskonstellationen und Vertragstypen zwischen Plattformbetreibenden, Herstellern und Kundinnen und Kunden zustandekommen können und welche Auswirkungen das jeweils hat, wurde in Kapitel 3.1. dargestellt. Wenn sich die Beteiligten nicht an die vereinbarten Regeln halten, kommt eine vertragliche Haftung in Betracht, also meist eine Geldzahlung. Plattformbetreibende und Hersteller können manchmal selbst eine solche Haftung fordern oder Adressat einer solchen Haftung werden. Dagegen können sie sich durch bewusste Ausgestaltung der Verträge und Einhaltung der Gesetze absichern.

Manchmal wird im Vertrag selbst geregelt, was bei einem Verstoß geschehen soll. Es könnte etwa vereinbart werden, dass die Kundin oder der Kunde einen bestimmten Betrag erhält, wenn durch ein Logistikunternehmen trotz der eingebauten Sensorik nicht angezeigte Schäden der Waren entstehen. Eine solche Vereinbarung kann ein Anreiz für Kundinnen und Kunden sein, ein bestimmtes Vertragsangebot anzunehmen. Allerdings sollten Plattformbetreibende oder Hersteller auch nur das zusichern, was sie sicher einhalten können.

Bei einigen Vertragsarten legt das Gesetz die Ersatzleistungen und deren Voraussetzungen bzw. die Voraussetzungen für Schadensersatz fest.

Nicht immer werden aber alle Eventualitäten vertraglich geregelt. Wenn sich keine vertraglichen Vereinbarungen und auch keine speziellen gesetzlichen Regelungen zu einem bestimmten Vertragsverstoß finden, heißt das nicht, dass für den Verstoß nicht gehaftet werden muss. Im Gegenteil, dann greift die allgemeine Regelung über vertragliche Pflichtverletzungen: Nach § 280 BGB muss die Partei, die den Vertrag nicht einhält, für einen dadurch erlittenen Schaden grundsätzlich Ersatz leisten. Nur wenn sie beweisen kann, dass sie die Pflichtverletzung nicht verschuldet hat, haftet sie nicht.

Es kann nicht nur für die Verletzung von Hauptpflichten des Vertrages, also etwa das Bereitstellen der Plattform oder Warenlieferung, sondern auch für die Verletzung von Nebenpflichten gehaftet werden. Das kann die Aufklärung über Risiken des Produkts sein oder der Schutz vor Missbrauch – etwa vor Betrügerinnen oder Betrügern, die auf der Plattform tätig sind. Auch die eigene Mitwirkung bei der Erfüllung der Hauptpflicht durch die andere Partei gehört dazu, zum Beispiel durch Bereitstellen bestimmter Informationen für die Plattform. Ob im konkreten Fall Nebenpflichten bestehen bzw. wie weit sie reichen, ist oft schwierig zu bestimmen. Hier spielen neben der Auslegung des Vertrags auch die Üblichkeiten des jeweiligen Verkehrskreises bzw. der jeweilige Vertragstyp eine Rolle. Für kollaborative Geschäftsmodelle und das Betreiben von Plattformen ist problematisch, dass die Konstellationen neuartig sind und deshalb noch keine gewachsenen Üblichkeiten existieren.

Plattformbetreibende Unternehmen sollten deshalb bei der Einhaltung und Interpretation der Nebenpflichten eher vorsichtiger als zu nachlässig sein. Dazu gehört zum Beispiel, das Bewertungssystem auf der Plattform neutral zu gestalten.[27] Außerdem darf das betreibende Unternehmen die Bewertungen auf der Plattform nicht erfinden, manipulieren oder vor Veröffentlichung kontrollieren. Sollte es gegen diese Pflichten verstoßen, haftet es der geschädigten Person oder Partei gegenüber. Das gilt sogar dann, wenn es mit dem oder der Geschädigten selbst keinen Vertrag abgeschlossen hat (deliktische Haftung).

27 Engert, AcP 218 (2018), 304, 376.

Die vertragliche Haftung beginnt nicht immer erst mit dem Abschluss des Vertrags, sondern kann in manchen Fällen schon vorher greifen.[28] Das ist für Plattformen von Bedeutung, da sie ja gerade der Vertragsanbahnung dienen. Die vorvertragliche Haftung betrifft dabei aber nur diejenigen, zwischen denen sich im konkreten Fall ein Vertrag anbahnt. Eine vorvertragliche Pflicht könnte verletzt werden, wenn Anbieter unzutreffende Informationen einstellen, auf die sich Nutzerinnen und Nutzer verlassen, und dann in Annahme der Richtigkeit dieser Angaben andere Anbieter bei einer Auswahl nicht berücksichtigen. Werden diese Pflichten verletzt, können Anbieter dafür haften.

Zudem können die AGB des plattformbetreibenden Unternehmens durch Auslegung in den Vertrag zwischen Nutzerinnen und Nutzern einbezogen werden.[29] Wenn dies aber dazu führt, dass unwirksame AGB in den Vertrag Eingang finden, so verletzt das plattformbetreibende Unternehmen vorvertragliche sowie, wenn es selbst einen Vertrag abgeschlossen hat, vertragliche Nebenpflichten und haftet für alle Schäden, die daraus entstehen.[30]

3.2.4 Möglichkeiten des Haftungsausschlusses (in AGB)

Eine Haftung kann grundsätzlich vertraglich ausgeschlossen oder zumindest begrenzt werden. Auch Plattformbetreibende oder Hersteller können in Verträgen festlegen, für bestimmte Fehler oder Schäden nicht haften zu wollen. Diesen Möglichkeiten sind jedoch gesetzliche Grenzen gesetzt. Werden Haftungsbeschränkungen und -ausschlüsse in AGB festgelegt, darf die andere Vertragspartei z. B. nicht unangemessen benachteiligt werden. Zudem darf nicht gegen wesentliche Grundgedanken des Vertrags verstoßen werden; das wäre etwa der Fall, wenn das plattformbetreibende Unternehmen in den AGB festlegt, dass es die Bewertungen auf seiner Plattform ohne Weiteres manipulieren oder vorkontrollieren darf. Auch gilt es zu bedenken, dass die jeweilige AGB-Vereinbarung nur dann Anwendung findet, wenn zwischen den Parteien ein Vertrag wirksam zustande gekommen ist und die AGB auch Bestandteil dieses Vertrags wurden (vgl. oben, 3.1.2). In § 309 Abs. 1 Nr. 5, 7, 8, 12 BGB finden sich außerdem detaillierte Regeln zur Pauschalisierung von Schadensersatzansprüchen, zum Haftungsausschluss bei Verletzung von Leben, Körper, Gesundheit und bei grobem Verschulden, zu sonstigen Haftungsausschlüssen bei Pflichtverletzung und zur Beweislast.

Bevor Plattformbetreibende oder Hersteller also die Haftung in ihren Verträgen ausschließen, mindern oder dazu detaillierte Bestimmungen treffen wollen, sollten sie diese Regelungen im Einzelnen durchgehen und, am besten mit anwaltlicher Beratung, die Grenzen ermitteln.

Natürlich können durch einen Haftungsausschluss oder eine Begrenzung finanzielle Risiken gesenkt werden. Zugleich ist immer auch zu beachten, dass das Vertrauen der Kundinnen und Kunden in eine Ware oder Dienstleistung tendenziell eher erhöht wird, wenn Anbieter oder Plattformbetreibende ihre Haftung gerade nicht reduzieren, sondern selbst durch Übernahme der Verantwortung ihr Vertrauen in das Produkt oder ihr Angebot zeigen. Es kann also ein Wettbewerbsvorteil sein, Haftung zu übernehmen.

28 Culpa in Contrahendo, geregelt in § 311 i.V.m. §§ 280, 241 BGB.
29 Mittlerweile ständige Rechtsprechung; vgl. etwa BGH NJW 2017, 468, 469 m.w.N.
30 §§ 280 Abs. 1, 241 Abs. 2 und gegebenenfalls 311 Abs. 2 BGB; Engert, AcP 218 (2018), 304, 351; Omlor, jM 2017, 134, 139.

3.2.5 Deliktische Haftung[31] (kein Vertrag)

Zusätzlich kann auch deliktisch gehaftet werden, wenn zwischen den Betroffenen kein Vertrag besteht oder das Verhalten nicht vom Vertrag erfasst ist. Wenn etwa ein Produkt, das auf einer Plattform entwickelt wurde, später Unbeteiligte schädigt, könnten alle an der Entwicklung Beteiligten und möglicherweise das plattformbetreibende Unternehmen selbst auch deliktisch haften. Aber auch schon vorher können Schadensereignisse auftreten, etwa wenn eine Anwenderin oder ein Anwender einer Anlage, die auf einer Engineering-Plattform entwickelt wurde, durch eine Fehlsteuerung verletzt wird. Gerade, weil in vielen Fällen keine eigene vertragliche Beziehung zwischen den Betroffenen entsteht, ist die deliktische Haftung bei kollaborativer Tätigkeit von erheblicher Bedeutung.

Zu beachten ist grundsätzlich, dass – soweit doch ein Vertrag abgeschlossen wurde – in den Grenzen der „guten Sitten“ auch ein Ausschluss der deliktischen Haftung möglich ist.[32] Dies gilt jedoch nur für fahrlässiges Verhalten, nicht aber für vorsätzliches Handeln.[33] Ein Ausschluss der Verschuldenshaftung hinsichtlich der Rechtsgüter Leben, Körper und Gesundheit durch AGB ist unzulässig; bei Sachbeschädigung ist nur ein Ausschluss leichter Fahrlässigkeit zulässig.[34] Das heißt, dass bei einem vertraglichen Ausschluss einer Haftung auch diese Grenzen bei der Vertragsgestaltung zu beachten sind, damit der Vertrag insgesamt wirksam und das Risiko der Haftung von vorneherein zumindest zum Teil kalkulierbar bleibt.

Die zentrale Vorschrift für deliktische Haftung ist § 823 Abs. 1 BGB. Sie bestimmt, dass wer rechtswidrig und schuldhaft Leben, körperliche Unversehrtheit, Freiheit oder Eigentum eines anderen verletzt, für den entstandenen Schaden haftet. So könnte etwa ein Teil, dass das fehlerhafte Ergebnis eines 3-D-Drucks ist, in einer Maschine eingebaut werden, die anschließend versagt und jemanden verletzt.

Geschützt vor einer Verletzung werden zudem sonstige Rechte, die in der ein oder anderen Konstellation für kollaborative Geschäftsmodelle relevant sein können: Software,[35] die nicht auf einem Datenträger, sondern etwa in der Cloud o. ä. gespeichert ist; das Recht am eingerichteten und ausgeübten Gewerbebetrieb, etwa wenn aufgrund einer fehlerhaften Lieferung o. ä. die Produktion nicht mehr weiterlaufen kann[36]; das allgemeine Persönlichkeitsrecht und Recht auf informationelle Selbstbestimmung sowie Recht am eigenen Bild (je nach Tätigkeit und Informationsdarstellung auf der Plattform). Nicht erfasst sind reine Vermögensschäden, das heißt, dass finanziell nachteilige Transaktionen allein keinen Schadenersatz begründen können.

Ein Schadenersatz kommt bei all diesen Schädigungen immer nur in Betracht, wenn der Schaden zurechenbar und „rechtswidrig und schuldhaft“ verursacht wurde. Meist geht es im Geschäftsverkehr dabei um fahrlässiges Handeln – das bedeutet, um eine mögliche Haftung zu verhindern, muss gewusst werden, wann die Fahrlässigkeit beginnt und diese Grenzen einhalten werden. Grundsätzlich liegt Fahrlässigkeit vor, wenn die im Verkehr erforderliche Sorgfalt nicht eingehalten wird. Dabei wird auf den jeweiligen Verkehrskreis

31 Zur deliktischen Haftung im Kontext von KI vgl. Eichelberger, Zivilrechtliche Haftung für KI und smarte Robotik, in: Ebers/Heinze/Krügel/Steinrötter, Künstliche Intelligenz und Robotik - Rechtshandbuch, erscheint voraussichtlich im September 2020.
32 Diese Grenzen sind in §§ 138 und 242 BGB normiert.
33 Vgl. § 276 Abs. 3 BGB.
34 § 309 Nr. 7 lit. a und b BGB.
35 BeckOGK/Spindler, 1.8.2019, BGB § 823 Rn. 136 ff.
36 Das gilt aber nur, wenn ein zielgerichteter, betriebsbezogener Eingriff auf den Gewerbebetrieb erfolgt, d. h. der Eingriff gegen den Betrieb als solchen und nicht gegen davon ablösbare Rechte/Güter gerichtet war.

der handelnden Partei abgestellt. Indizien für den Sorgfaltsmaßstab sind Rechtsnormen oder nicht-staatliche Normen (ISO/DIN). Allerdings kann ein Gericht von solchen Normen im Einzelfall abweichen, etwa wenn sie veraltet sind. Für jeden Lebensbereich gibt es spezielle Vorgaben und detaillierte Rechtsprechung zu der jeweils erforderlichen Sorgfaltspflicht. So gehört es wie erwähnt beispielsweise zur Pflicht eines plattformbetreibenden Unternehmens, Neutralität bezüglich der Bewertungen zu wahren. Wenn es bestimmte Bewertungen bevorzugt darstellt, ohne dies transparent zu machen, wäre es haftbar für jeden Schaden, der einer Nutzerin oder einem Nutzer daraus entsteht.

Für kollaborative Geschäftsmodelle spielt bei der Ermittlung der Sorgfaltspflicht auch eine Rolle, ob Plattformbetreibende oder Systemintegratoren als vermittelnde oder als herstellende Unternehmen auftreten:

Wer selbst als Anbieterin oder Anbieter auftritt und ggf. nur einzelne Aufträge an Subunternehmen delegiert, haftet umfassend – gegebenenfalls auch im Rahmen der Produzenten- und Produkthaftung (vgl. unten).

Wenn die Plattform nur der Vermittlung dient, zeigt das betreibende Unternehmen damit, dass es für die Angebote nicht verantwortlich sein möchte. Das schließt die Verantwortung allerdings nur teilweise aus: Es muss dennoch aktiv werden, wenn es von Tatsachen, die für Leib, Leben oder Gesundheit potenzieller Nutzerinnen und Nutzer von erheblicher Bedeutung sind, positive Kenntnis erlangt. Es beabsichtigt ja gerade, dass verschiedene Personen auf seiner Plattform Kontakt aufnehmen und hat außerdem über die Bewertungen die beste Möglichkeit, über solche Vorgänge Kenntnis zu erhalten. Deshalb ist es für die Personen, die diese Plattform nutzen, dann auch zumindest insoweit verantwortlich.

Unterfall: Produzentenhaftung[37]

Werden im Rahmen von kollaborativen Geschäftsmodellen Produkte hergestellt und in Verkehr gebracht, greifen besondere Haftungsregeln: Zum einen die Produzentenhaftung, zum anderen die Produkthaftung (später unter 3.2.6).

„Produzentenhaftung" meint eine besondere Form der deliktischen Haftung, bei der gerade die für die Produzierenden wichtigen Sorgfaltspflichten herausgestellt werden. Produzierende in diesem Sinne sind Hersteller von beweglichen Sachen und von Software und ggf. auch Erbringerinnen und Erbringer von Dienstleistungen. Für Plattformbetreibende gelten diese Besonderheiten dann, wenn sie selbst als entwickelndes bzw. herstellendes Unternehmen auftreten, nicht aber, wenn nur Vermittlertätigkeiten angeboten werden.

Sorgfaltsmaßstab: Jeder Hersteller bzw. Anbieter muss bei seiner Tätigkeit die im Verkehr erforderliche Sorgfalt aufwenden.[38] Der konkrete Inhalt dieser Pflicht hängt von vielen Faktoren ab und ist im Einzelfall zu bestimmen. Zu berücksichtigen sind dabei: Gebrauchs- und Sicherheitserwartungen der Abnehmerinnen und Abnehmer; Kreis der Abnehmerinnen und Abnehmer; Art, Umfang und Häufigkeit der mit der Nutzung des Produkts verbundenen Risiken und Gefahren. Gerade bei neuartigen Produkten und Vorgehensweisen fehlt es oft an konkreten Maßstäben – wenn es aber Maßstäbe bezüglich der konkreten Anwendungen gibt, sind diese zu beachten (etwa bei Medizinprodukten o. ä.). Da die folgenden Pflichten

37 Vgl. hierzu Eichelberger, Rn. 6 ff.
38 Eichelberger, Rn. 12 ff.; BGH Urt.v.17.101989 – VI ZR 258/88, NJW 1990, 906 (907) – Pferdeboxen.

gerade mit Blick auf Hersteller (und das gilt auch für als solche agierenden Plattformen) entwickelt wurden, ist es wichtig, diese Pflichten zu kennen und zu befolgen:

Konstruktionspflichten:
Bei Konzeption und Planung jedes Produkts sind alle Maßnahmen zu treffen, die zur Vermeidung einer Gefahr objektiv erforderlich und nach objektiven Maßstäben zumutbar sind.[39] Dabei muss sich am neuesten Stand der Wissenschaft und Technik orientiert werden. Dieser Maßstab gilt auch bei der Entwicklung von Software. So gilt es klassische Programmierfehler zu vermeiden, etwa die fehlende Vorsorge gegen einen Ausfall oder eine Fehlfunktion, aber auch unzureichende Sicherung gegen Angriffe von außen. Ein Sonderproblem ist, wie bei Automatisierung (etwa bei der Robotik) mit fehlerhaften „Lernprozessen" umzugehen ist.[40] Wenn das Produkt bei Herstellung bereits mit fehlerhaft „Erlerntem" ausgestattet wird, ist das ein Konstruktionsfehler. Wenn aber die Weiterentwicklung an sich nicht fehlerhaft, sondern nur die Ergebnisse unerwartet oder unerwünscht sind, ist nicht ohne Weiteres von einem Konstruktionsfehler auszugehen. Der Hersteller muss aber erwartbare Verhaltensweisen der anwendenden Personen einbeziehen. Zudem könnte es bei kollaborativ entwickelten Produkten und neuartigen Interaktionsformen notwendig sein, die Vorgehensweise und die Produkte unter Realbedingungen zu testen und dabei zu beobachten.

Instruktionspflichten:
Ein Hersteller muss Anwendende von Produkten sorgfältig instruieren, d. h. vor allem vor möglichen Gefahren bei der Verwendung warnen und Vermeidungsmöglichkeiten aufzeigen. Diese Pflichten können herabgesetzt werden, wenn es sich bei den Anwendenden um Fachpersonen handelt.

Produktbeobachtungspflichten[41]:
Ein Hersteller muss ein Produkt nach Inverkehrbringen mit Blick auf danach entstehende Gefahren beobachten und gegebenenfalls Maßnahmen zur Bekämpfung treffen. Das gilt gerade bei komplexen Neuentwicklungen mit großem Schädigungspotential, wie sie bei der Umsetzung von kollaborativen Geschäftsmodellen entstehen können. Bei Systemen, die noch mit dem Hersteller vernetzt sind, ist eine Beobachtung unproblematisch möglich und somit meistens auch zumutbar. Oft gehört es schon zur Konstruktionspflicht, eine Vernetzung und damit Beobachtungsmöglichkeiten in die Produkte zu integrieren – so wie es in einer bestimmten Weise ja auch im Bereich der Logistik gehandhabt wird. Die Beobachtungspflicht ist grundsätzlich zeitlich unbeschränkt, kann sich aber abschwächen. Problematisch ist, dass der Hersteller möglicherweise nicht für die gesamte Lebensdauer des Produkts existiert. In solchen Fällen kann es sein, dass Pflichten auf Betreibende/Anwenderinnen und Anwender verlagert werden („TÜV") oder dass Hersteller zu Maßnahmen verpflichtet sind, die die Sicherheit auch für die Zukunft gewährleisten. Zu beachten ist zudem, dass die Beobachtungspflicht auch bezüglich Daten und Leistungen Dritter bestehen kann, auf denen das Produkt aufbaut. Sollten Gefahren auftreten, muss der Hersteller die Abnehmerinnen und Abnehmer bzw. die Öffentlichkeit vor diesen warnen oder, in besonders schweren Fällen, das Produkt zurückrufen. Bei Softwarefehlern kommt auch eine Fehlerbeseitigung über das Internet o. ä. in Betracht (z. B. durch ein Update).

39 Eichelberger Rn. 21; BGH Urt. v. 16.6.2009 – VI ZR 107/08, BGHZ 181, 253 = NJW 2009, 2952 Rn. 15.
40 Hierzu und zum Folgenden Eichelberger, Rn. 23 ff.
41 Eichelberger Rn. 32 ff.

Haftung wegen Verstößen gegen Schutzgesetze

Nach § 823 Abs. 2 BGB wird für Schäden gehaftet, die daraus entstehen, dass gegen ein Schutzgesetz verstoßen wird, etwa das Produktsicherheitsgesetz oder das Medizinproduktegesetz. Das kann für kollaborative Geschäftsmodelle relevant werden, wenn Produkte entwickelt werden, für die solche Gesetze einschlägig sind. Da hier nicht alle Schutzgesetze dargestellt werden können, ist hier für Plattformbetreibende und Hersteller wichtig, sich über die relevanten Spezialgesetze zu informieren und zu prüfen, ob ihre Produkte darunterfallen, um dann diese Gesetze sorgfältig einzuhalten.

Schädigung durch mehrere Personen/kollaboratives Zusammenwirken

Die Schädigung wird gerade bei kollaborativen Geschäftsmodellen oft nicht nur durch einen der Beteiligten, sondern erst durch das Zusammenwirken mehrerer Beteiligter herbeigerufen. Solange diese keine juristische Person gegründet haben[42], haftet grundsätzlich jeder Beteiligte selbst für seinen eigenen Beitrag. Für jeden dieser Beiträge ist also darauf zu achten, ob er ursächlich und zurechenbar zur Schädigung geführt hat – oder andersherum sollte jeder Beteiligte darauf achten, dass sein eigener Beitrag eben zu keiner Schädigung führt und er sich sorgfaltsgemäß verhält.

Es treten aber bei Kollaborationen auch einige Besonderheiten auf: So spielt beim Ermitteln der Sorgfaltspflicht hier der sogenannte „Vertrauensgrundsatz" eine Rolle. Außerdem kann es vorkommen, dass man für „Verrichtungsgehilfen" haftet. Gelegentlich haftet man auch mit anderen gemeinsam; dann stellt sich die Frage nach dem Umgang mit Schuldnermehrheiten.

Vertrauensgrundsatz bei Kollaborationen und Kooperationen

Der Vertrauensgrundsatz besagt, dass sich bei (gleichrangigen) Kooperationen grundsätzlich darauf verlassen werden darf, dass sich die anderen Beteiligten ordnungsgemäß verhalten. Weder als plattformbetreibendes noch als herstellendes Unternehmen[43] muss man also per se mögliche Fehler anderer in sein Verhalten einbeziehen. Das gilt allerdings nur solange, wie sich keine Anhaltspunkte für das Gegenteil finden. Ist aber erkennbar, dass sich andere nicht sorgfaltsgemäß verhalten, dann darf man darauf nicht mehr vertrauen. Das wäre etwa der Fall, wenn man in der Zusammenarbeit schon mehrere Male schlechte Erfahrungen mit anderen gemacht hat oder auch wenn auf einer Plattform einige negative Rückmeldungen kamen (und diese plausibel erscheinen). In diesem Fall muss man entweder eine zuverlässigere Partnerschaft suchen oder die möglichen Fehler vorab berücksichtigen.

Haftung für Verrichtungsgehilfen (vermutetes Verschulden)

Das Zivilrecht sieht in § 831 Abs. 1 BGB die Haftung für Verrichtungsgehilfen vor. Hiernach haftet man dafür, dass man andere zu einer Verrichtung, zu der man eigentlich selbst verpflichtet wäre, bestellt und diese bei dieser Verrichtung Dritte schädigen. Das gilt nur dann nicht, wenn man nachweisen kann, dass bei der Auswahl, der Überwachung und der Anleitung von Verrichtungsgehilfen sorgfaltsgemäß gehandelt wurde, d. h. bei der Auswahl, Beschaffung erforderlicher Vorrichtungen und Gerätschaften sowie der Leitung der Verrichtung die im Verkehr erforderliche Sorgfalt beobachtet wurde oder der Schaden auch bei Beobachtung eingetreten wäre (Abs. 1 S. 2). Aber auch wenn man sorgfaltswidrig gehandelt hat, kann man der Haftung entgehen, wenn feststeht, dass der Schaden auch bei Einhaltung der Sorgfaltspflicht eingetreten wäre. Diese Art der Haftung ist etwa bei eigenständig auftretenden Systemintegratoren denkbar, wenn sie die Erfüllung ihrer Pflichten auf Dritte delegieren, aber selbst als Lieferanten gegenüber Kundinnen und Kunden auftreten. Ähnliches gilt auch für Plattformen, die als Hersteller auftreten und selbst die verschiedenen Beteiligten aussuchen.

42 Etwa eine Gesellschaft des bürgerlichen Rechts, GbR, §§ 705 ff. BGB.

43 Daneben kommt aber immer auch Produkthaftung in Betracht; hier haftet ein Hersteller unabhängig von seinem konkreten Beitrag für Schäden, die durch das von ihm vertriebene Produkt verursacht werden.

Schuldnermehrheiten/Gesamtschuld

Bei kollaborativen Geschäftsmodellen wird es also nicht selten vorkommen, dass mehrere Personen gleichzeitig haften. Normalerweise haftet jeder für den eigenen Beitrag. Das gilt dann nicht, wenn die Beteiligten nach außen hin miteinander verbunden auftreten und den Gläubigern auf gleicher Stufe zu einer gleichartigen Schuld verpflichtet sind. Dann handelt es sich um Gesamtschuldner (§ 421 BGB). Gläubiger können dann von jedem Schuldner die ganze Leistung verlangen und die entsprechende Aufteilung muss anschließend von den Schuldnern untereinander im Innenverhältnis geklärt werden.

3.2.6 Gefährdungshaftung

Neben der Haftung für eine „schuldhafte" Schädigung anderer gibt es die Gefährdungshaftung. Das bedeutet, dass man schon dafür haftet, dass Dritte durch ein eigenes Verhalten einem Risiko ausgesetzt werden und sich dieses Risiko in einer Schädigung verwirklicht. Denn die Gesetzgebung hat sich in diesen Fällen dafür entschieden, das Risiko eben nicht Dritten aufbürden zu wollen, auch wenn die Gefährdung von der Gesetzgebung grundsätzlich als gesellschaftlich erlaubt angesehen wird. Dazu gehören etwa die Haftung für den Betrieb eines Kraftfahrzeugs (§ 7 StVG) oder die Haftung für ein Produkt nach dem Produkthaftungsgesetz (das ist zu unterscheiden von der oben dargestellten Produzentenhaftung).

Produkthaftung (ProdHaftG)

Die Produkthaftung schützt Endabnehmende eines Produkts sowie Unbeteiligte vor den Gefahren eines fehlerhaften Produkts, unabhängig von einem Vertrag oder einem Verschulden.[44] Die Haftung entsteht, wenn durch ein fehlerhaftes Produkt jemand getötet, in der Gesundheit geschädigt oder eine Sache beschädigt wurde. Das ist für Plattformbetreibende und Hersteller von besonderer Relevanz, da sie bei einer Produzenteneinstufung dieses Haftungsrisiko umfänglich tragen und mit den entsprechenden Maßnahmen vorbeugen müssen (das gilt für Hersteller grundsätzlich, für Plattformbetreibende dann, wenn sie als produzierende Unternehmen auftreten, vgl. hierzu sogleich unten).

Bezüglich der Sachbeschädigung ist an dieser Stelle zu beachten, dass es sich bei der beschädigten Sache um eine andere als die fehlerhafte Sache handeln muss und sie für den privaten Ge- oder Verbrauch bestimmt und dafür auch tatsächlich verwendet worden ist. Der Schaden muss durch ein Produkt hervorgerufen worden sein, d. h. jede bewegliche Sache sowie Elektrizität. Das Produkt muss fehlerhaft sein. Hierbei handelt es sich um eine schwierig zu bewertende Voraussetzung. Bei der Bewertung spielt unter anderem eine Rolle, wie und für welche Zwecke das Produkt angeboten bzw. beworben wurde bzw. welcher Gebrauch zu erwarten ist. Auch wenn es sich um eine Gefährdungshaftung handelt, trifft Geschädigte insofern eine gewisse Beweislast. Sie müssen Fehler, Schaden sowie Zusammenhang zwischen Fehler und Schaden beweisen.

44 Diese Haftung ist im ProdHaftG, für bestimmte spezielle Produkte außerdem im Arzneimittelgesetz (AMG), Medizinproduktegesetz (MPG) oder dem Lebensmittelgesetz (LMG) geregelt, die hier jedoch außen vor bleiben sollen.

Haftungsadressaten

Das Haftungsrisiko trifft vor allem die Hersteller, aber auch andere Beteiligte kommen als mögliche Haftungsadressaten in Betracht. Gerade bei kollaborativen Geschäftsmodellen sollte sich jede beteiligte Partei absichern, ob seine Beteiligung unter das ProdHaftG fällt und welche Konsequenzen das hat, bzw. ob man sich gegebenenfalls von der Haftung freizeichnen kann:

Hersteller: Hersteller haften, wenn Sie das Produkt erzeugt oder gewonnen haben.

Quasi-Hersteller: Als Herstellende haften aber auch diejenigen, die nach außen als Hersteller auftreten, d.h. wer sich durch das Anbringen seines Namens, seiner Marke oder eines anderen unterscheidungskräftigen Kennzeichens als herstellendes Unternehmen ausgibt.

Importierende: Auch wer das Produkt in den Europäischen Wirtschaftsraum einführt, gilt als Hersteller.

Lieferanten: Wenn der Hersteller nicht festgestellt werden kann, gelten Lieferanten als Hersteller. Sie können sich jedoch von der Haftung befreien, wenn sie Geschädigten innerhalb eines Monats, nachdem ihnen deren diesbezüglichen Aufforderungen zugegangen sind, den Hersteller oder diejenigen Personen benennen, die ihnen das Produkt geliefert hat.

Aufteilung der Haftung

In Konstellationen der kollaborativen Herstellung von Produkten auf Plattformen kommen häufig mehrere (natürliche oder juristische) Personen als Hersteller und damit als Haftungsadressaten in Betracht. Diese haften gesamtschuldnerisch (§ 5 S. 1 ProdHaftG), die Folgen wurden bei der deliktischen Haftung dargestellt. Etwas Anderes gilt nur, wenn der Schaden eindeutig durch Fehler eines Endherstellers verursacht wurde: Dann haftet nur dieses.

Umfang der Haftung

Im Gesetz finden sich auch Bestimmungen zum Haftungsumfang. Bei Personenschäden ist die Haftung für ein Schadensereignis bezüglich aller Personen auf 85 Millionen Euro begrenzt. Für die Haftung wegen der Beschädigung einer Sache gilt eine Selbstbeteiligung (500 Euro). Die Haftung wird gemindert, wenn den Geschädigten ein Mitverschulden trifft.

Haftungsausschluss

Das ProdHaftG schließt zudem unter bestimmten Bedingungen die Haftung aus – wobei das immer nur für die Haftung gerade nach dem ProdHaftG gilt. So haftet nicht nach dem ProdHaftG, wer das Produkt nicht in Verkehr gebracht hat, d. h. es nicht an andere überlassen hat – das ist etwa der Fall, wenn das Produkt gestohlen wurde oder nur zum Zweck der Erprobung oder Prüfung übergeben wurde. Die Haftung nach diesem Gesetz ist auch ausgeschlossen, wenn nach den Umständen davon auszugehen ist, dass der Fehler des Produkts zum Zeitpunkt des Inverkehrbringens noch nicht vorlag. Ein Haftungsausschluss

wird auch begründet, wenn das Produkt weder für den Verkauf/Vertrieb hergestellt noch im Rahmen einer beruflichen Tätigkeit hergestellt oder vertrieben wurde. Die Haftung ist weiterhin ausgeschlossen, wenn der Fehler darauf beruht, dass das Produkt zwingenden Rechtsvorschriften entsprochen hat oder der Fehler nach dem Stand der Wissenschaft und Technik zum Zeitpunkt des Inverkehrbringens nicht erkannt werden konnte. Schließlich finden sich Ausschlussgründe für Hersteller von Teilprodukten und Grundstoffen. Von Bedeutung ist, dass der Hersteller die Voraussetzungen des Ausschlussgrundes beweisen muss.

3.2.7 Strafrechtliche Verantwortung

Haftung erfasst auch die strafrechtliche Verantwortung von Beteiligten. Bei kollaborativen Geschäftsmodellen kommt eine solche bei Schädigungen von Plattformnutzenden, Beteiligten der Wertschöpfungskette (oder dessen Angestellten), Käuferinnen und Käufer eines kollaborativ hergestellten Produkts oder gar gänzlich Unbeteiligten in Betracht. Denkbar sind insbesondere Strafbarkeiten wegen fahrlässiger Tötung oder fahrlässiger Körperverletzung (§ 222 StGB und § 229 StGB).

Für Plattformbetreibende und Hersteller ist das Risiko einer solchen Haftung besonders zu beachten, da man strafrechtlich immer persönlich haftet, hiergegen auch keine Versicherung möglich ist und einen erhebliche Folgen (Geld- oder Freiheitsstrafe) treffen können. Deshalb ist eine Absicherung gegen dieses Risiko besonders sorgsam zu treffen.

Strafbar macht man sich dann, wenn man durch eine Handlung ein rechtlich relevantes Risiko dafür geschaffen hat, dass ein anderer Mensch getötet oder verletzt wird und sich auch genau dieses Risiko verwirklicht. Neben anderen Voraussetzungen ist bei kollaborativen Geschäftsmodellen bedeutsam, ob die Handlung fahrlässig war, d. h. gegen strafrechtliche Sorgfaltspflichten verstoßen hat. Der Sorgfaltsmaßstab wird wiederum bestimmt mit Blick darauf, wie sich ein gewissenhafter und besonnener Mensch aus dem Verkehrskreis der Täterin oder des Täters in der konkreten Lage verhalten hätte. Dabei spielen geschriebene und ungeschriebene Regelungen eine Rolle, also Rechtsnormen oder auch nicht-rechtliche Regelungen (DIN- oder ISO-Normen). Gerade bei Letzteren ist aber zu beachten, dass diese Normen nur ein Indiz für den Sorgfaltsmaßstab sind, die Gerichte aber jederzeit auch von derartigen nicht-staatlichen Normen abweichen können (z. B. wenn sie veraltet sind). Anschließend sind ungeschriebene Regeln wie Verkehrsgepflogenheiten oder anerkannte Erfahrungssätze (Regeln der Technik) zu prüfen. Gerade in einem relativ neuen Wirtschaftsbereich wie dem Plattformbetrieb sind Sorgfaltsmaßstäbe nur schwer zu ermitteln. Genau dann ist (wie oben dargelegt) auf den besonnenen „Durchschnittsmenschen“ aus dem jeweiligen Verkehrskreis abzustellen. Dieser ist im Zweifelsfall sicherlich schwer zu ermitteln, es ist jedoch auch zu beachten, dass gerade im Strafrecht nur klare Verstöße zu einer Haftung führen. Für Plattformbetreibende und Hersteller gilt: Eine Orientierung an den Üblichkeiten im konkreten Wirtschaftsbereich ist ebenso wichtig wie der Nachweis, dass man möglichst viele (zumutbare) Maßnahmen zur Vermeidung von Gefahren, insbesondere für Unbeteiligte, getroffen hat.

Risikomanagement (insbesondere im GmbH- und Aktienrecht)

Alle im Geschäftsverkehr tätigen Unternehmen sind generell mit Blick auf bestimmte Risiken zu präventivem Management verpflichtet und haften (z. T. auch als persönliche Haftung) wenn sie dem nicht ordnungsgemäß nachkommen. Somit sollten Plattformbetreibende und Hersteller auch das entsprechende Risikomanagement im Blick haben.

Das gilt etwa dann, wenn sie als GmbH oder als AG agieren: Grundsätzlich richtet sich die Haftung der GmbH nach den allgemeinen Regeln, sie haftet jedoch nur für ihre eigenen Verbindlichkeiten, nicht für die ihrer Gesellschafterinnen oder Gesellschafter. Zudem haftet sie nur mit dem Gesellschaftsvermögen. Diese Beschränkung wird unter bestimmten Voraussetzungen durchbrochen, sodass auch die Gesellschafterinnen oder Gesellschafter unmittelbar haften („Durchgriffshaftung"). Dazu gehören Rechtsformmissbrauch, Vermögens- und Sphärenvermischung und materielle Unterkapitalisierung. Ein weiteres Risiko ist die „Haftung in der Gründungsphase". Nach § 91 Abs. 2 AktG und dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) müssen Unternehmen eine Risikofrüherkennung bezüglich ihrer Existenz sicherstellen. Das gilt auch für andere Unternehmensformen wie die GmbH. Weiterhin müssen Aufsichtsräte die Finanzberichterstattung, Abschlussprüfung und Kontrollsysteme überwachen[45]. Für kapitalmarktorientierte Kapitalgesellschaften und gleichgestellte Personengesellschaften muss zudem transparent gemacht werden, wenn keine Risikofrüherkennung existiert, § 246a Abs. 1 HGB.

Risikomanagement bedeutet hier, vor allem die Risiken zu erkennen und abzuwenden, die die Existenz des Unternehmens bedrohen, insbesondere finanzwirtschaftliche Risiken, die zu Zahlungsunfähigkeit führen könnten (vgl. § 15 InsO). Deshalb gehört ein professionelles Controlling zu einem umfassenden, die persönliche Haftung ausschließenden Risikomanagement.

45 Vgl. hierzu das Bilanzmodernisierungsgesetz.

3.2.8 Verantwortung nach dem Telemediengesetz (TMG)

Für Plattformbetreibende ist mit Blick auf Haftung und Verantwortung auch das Telemediengesetz von großer Bedeutung. Adressaten der hier geregelten Verantwortung sind Internet-Provider, also Mittler zwischen den Nutzenden und Anbietenden im Internet. Das sind alle natürlichen oder juristischen Personen, die eigene oder fremde Telemedien zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln. Es ist zwischen verschiedenen Arten von Providern zu unterscheiden. So bietet ein Internet-Service-Provider nur die Einwahlmöglichkeit. Ein Internet-Presence-Provider bietet Speicherplatz und Serverfunktionen. Zu differenzieren ist weiterhin nach Content-Provider, Host-Provider, Access-Provider (s. unten) oder Link-Anbieter, auch Plattformbetreibende fallen darunter.

Das TMG regelt in §§ 7-10 Voraussetzungen der Provider-Haftung, die für alle Rechtsgebiete gelten, also auch die zivilrechtliche und strafrechtliche Haftung. Geregelt werden jedoch nicht alle Haftungsfragen, sondern die Frage, inwieweit Provider für rechtswidrige Inhalte auf Websites, die von ihnen betrieben oder technisch betreut werden, rechtlich verantwortlich sind. Das TMG privilegiert verschiedene Provider je nach ihrem Angebot und ihren Möglichkeiten.

Content-Provider = wer eigene Inhalte auf eine Website stellt: Dieser ist für diese Inhalte voll verantwortlich.

Host-Provider = wer fremde Inhalte auf seinem Server/Websites einstellt (nach außen muss deutlich werden, dass es sich um ein fremdes Angebot handelt): Dieser haftet grundsätzlich nicht für fremde Inhalte. Er haftet aber, wenn er positive Kenntnis von rechtswidrigen Inhalten hatte und nichts dagegen unternommen bzw. sie nicht gelöscht hat. Grundsätzlich ist er ohne positive Kenntnis von rechtswidrigen Inhalten nicht zur Überwachung verpflichtet.

Access-Provider = wer fremde Inhalte im Netz vermittelt oder durchleitet oder nur den Zugang zum Internet ermöglicht: Dieser haftet grundsätzlich nicht für fremde Inhalte, wenn er die Übermittlung nicht veranlasst, die Adressaten oder den Adressaten der Inhalte nicht ausgewählt und die übermittelten Inhalte nicht ausgewählt oder verändert hat.

Usenet-Provider = wer Netzwerke von Diskussionsforen betreibt: Dieser haftet nach der Rechtsprechung[46] als Cache-Provider.

Für Plattformbetreibende, die nur vermittelnd agieren, gilt grundsätzlich, dass keine Überprüfungspflicht besteht. Sie haften für auf der Webseite veröffentlichte Informationen nur, soweit es sich um eigene oder zu eigen gemachte fremde Informationen handelt.[47]

Aktuelle Diskussionen und Neuregelungen

Schon seit einer Weile wird intensiv darüber diskutiert, ob es für Betreibende von Plattformen neuer Haftungsregelungen bedarf.[48] Nun ist zum 12. Juli 2020 eine neue EU-Verordnung in Kraft getreten (Platform-To-Business).[49] Diese Verordnung dient dazu, die Rechte von Unternehmen zu stärken, wenn sie Plattformen nutzen. Entsprechend müssen sich Plattformbetreibende für die Zukunft an die Neuregelungen halten, die bestimmte einseitige und wettbewerbswidrige Machtausübungen ihrerseits eindämmen sollen. Die Parameter für Rankings auf der Plattform müssen in AGBs niedergelegt sein, ebenso, ob dies durch Entgeltzahlungen beeinflussbar ist. Für Einschränkung, Aussetzen oder Beendigung des Zugangs zur Plattform ist ein effektives Beschwerdemanagement und ggf. Mediation erforderlich; auch die Informationen hierzu sind in den AGBs zu verankern. Zudem finden sich Regelungen zu Konstellationen, in denen Plattformbetreibende zusätzlich eigene Produkte auf der Plattform anbieten. Grundsätzlich betrifft die Verordnung also vor allem die Ausgestaltung der AGBs (vgl. oben). Die Verordnung gilt gegenüber gewerblichen Nutzenden, die ihren Sitz in der EU haben, wenn die Plattform dem Vertrieb von Waren oder Dienstleistungen an Kundinnen und Kunden in der EU dient. Viele Plattformen fallen deshalb nicht in den Anwendungsbereich der Verordnung, weil es sich um Business-to-Business-Plattformen handelt, bei denen eine Vermittlung an Endverbrauchende nicht angedacht ist. Dennoch sollten auch sie die Entwicklung der Gesetzgebung hin zu mehr Transparenz und Fairness auf Plattformen weiterhin beobachten.

48 Diskussionsentwurf für eine Richtlinie über Online-Vermittlungsplattformen, Research group on the Law of Digital Services, EuCML 2016, 164; Busch/Dannemann/Schulte-Nölke, MMR 2016, 787; Busch, in: De Francheschi (Hrsg.), European contract law and the Digital Single Market, 2016, 223, 234, 242 f.

49 Vgl. https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R1150&from=D [14.07.2020]

46 OLG Düsseldorf (Urt. v. 15.1.2008, Az. I-20 U 95/07); vgl. zu Internetversteigerungen BGHZ 158, 236 = GRUR 2004, 860 = CR 2004, 763 m. Anm. Volkmann = MMR 2004, 668; m. Anm. Hoeren: hier greift keine Privilegierung nach dem TMG, sondern eine Störerhaftung nach §§ 823, 1004 BGB analog. Die entsprechende Prüfungspflicht darf aber nicht ausufern, die Prüfung muss möglich und zumutbar sein (bzgl. der faktisch-technischen Gegebenheiten ist zu beachten, dass es kaum möglich ist, fremde Inhalte aus einem Usenet zu löschen).

47 Adam/Micklitz, in: Micklitz u. a. (Hrsg.), Verbraucherrecht 2.0 – Verbraucher in der digitalen Welt, 2017, 45, 58 ff.

3.3 IT-Sicherheit und Datenschutz

3.3.1 Technischer Datenschutz

Die Datenschutz-Grundverordnung[50] (DSGVO) stellt hohe Anforderungen an den Verantwortlichen[51] einer Verarbeitung von personenbezogenen Daten[52]. Werden die personenbezogenen Daten[53] zudem kollaborativ verarbeitet, wie es bei den PAiCE-Geschäftsmodellen durchgängig der Fall ist, steigt die datenschutzrechtliche Komplexität. Datenschutzrechtlich kommen die Modelle der Auftragsverarbeitung (Art. 28 DSGVO), der gemeinsamen Verantwortlichkeit (auch „joint controllers"/ „joint controllership", Art. 26 DSGVO) oder auch der getrennten Verantwortlichkeit (Art. 5 Abs. 1, 24 Abs. 1 DSGVO) in Frage. Die Modelle und deren datenschutzrechtlichen Anforderungen werden unten betrachtet.

Zentrale Norm für die Sicherheit der Datenverarbeitung in der DSGVO ist Art. 32. Diese Regelung sieht vor, dass Verantwortliche und Auftragsverarbeiter unter Berücksichtigung einer Vielzahl von gesetzlichen Aspekten geeignete technische und organisatorische Maßnahmen[54] zu treffen haben, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die (zwingend) zu berücksichtigenden Aspekte betreffen die Art, den Umfang, die Umstände und den oder die Zwecke der Verarbeitung sowie die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen. Die innerhalb von kollaborativen Geschäftsmodellen geplante Datenverarbeitung ist also am Maßstab der Rechte der betroffenen Personen – und nicht etwa anhand allein möglicher Angriffe auf die eingesetzte Informationstechnik – einer Schutzbedarfsanalyse zu unterziehen, die Grundlage für die einzusetzenden technischen und organisatorischen Maßnahmen ist. Zu berücksichtigen ist nach Art. 32 Abs. 1 DSGVO nunmehr auch der Stand der Technik.

Stand der Technik

Die DSGVO definiert den Stand der Technik nicht.[55] Der Stand der Technik kann als die im Waren- und Dienstleistungsverkehr verfügbaren Verfahren, Einrichtungen oder Betriebsweisen, deren Anwendung die Erreichung der jeweiligen gesetzlichen Schutzziele am wirkungsvollsten gewährleisten kann, dargestellt werden.[56] Verkürzt ausgedrückt: Der Stand der Technik bezeichnet die am Markt verfügbare Bestleistung von IT-Sicherheitsmaßnahmen zur Erreichung eines des/der gesetzlichen IT-Sicherheitsziele[57]. Diese Definition erlaubt eine handhabbare Abgrenzung zu Maßnahmen, die lediglich den allgemein anerkannten Regeln der Technik entsprechen und eben nicht die Speerspitze der Technologie repräsentieren. Maßnahmen nach dem Stand von Wissenschaft und Forschung können im Rahmen dieser Darstellung außer Betracht bleiben, da sie am Markt nicht verfügbar sind und somit weder operativ noch rechtlich unmittelbar relevant werden können.

50 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.
51 Definition s. Art. 4 Ziff. 7 DSGVO.
52 Siehe unten: Kollaborative Verarbeitung von Daten mit Personenbezug.
53 Definition s. Art. 4 Ziff. 1 DSGVO.
54 Mit technischen und organisatorischen Maßnahmen ist die Gesamtheit der Informationssicherheitsmaßnahmen gemeint. Zu den organisatorischen Maßnahmen zählen auch rechtliche Maßnahmen wie privatrechtliche Verträge (z. B. zum Datenschutz bzw. zur IT-Sicherheit oder zur Geheimhaltungsverpflichtung etc.)
55 Eine einschlägige nationale, gesetzliche Definition findet sich nicht und wäre auch nicht auf die EU-DSGVO unmittelbar anzuwenden. Lediglich in der Gesetzesbegründung zu § 8a BSIG bietet einen mit der o. g. Definition vergleichbaren Ansatz. Das vom Bundesverfassungsgericht noch in BVerfGE 49, 89 in Bezug genommene Begriffsverständnis trennt nicht definitorisch zwischen den subjektiven und objektiven Kriterien und ist somit im Rahmen der geltenden Normen bereits inhaltlich nicht anwendbar.
56 Bartels/Backer, Die Berücksichtigung des Stands der Technik in der DSGVO, DuD 4-2018, 214; Bartels/Backer/Schramm, Der „Stand der Technik" im IT-Sicherheitsrecht, Tagungsband zum 15. Deutschen IT-Sicherheitskongress 2017, Bundesamt für Sicherheit in der Informationstechnik, 503; Bartels/ Lawicki u.a., Handreichung zum „Stand der Technik" technischer und organisatorischer Maßnahmen, 2020-02, S. 11.
57 IT-Sicherheitsziele der DSGVO sind gem. Art. 32 Abs. 1 insbesondere die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit.

Das Berücksichtigungsgebot hinsichtlich des Stands der Technik bedeutet, dass der Stand der Technik nicht in jedem Fall zwingend umgesetzt werden muss.[58] Hier können die Beteiligten von Geschäftsmodellen von den vorgesehenen Spielräumen Gebrauch machen. Die Prüfung erfolgt zweistufig: Zunächst ist objektiv-technisch festzustellen, welche zur Erreichung bzw. Erhöhung der IT-Sicherheit in Betracht kommende Assets dem Stand der Technik entsprechen. Zur Bestimmung des Technologiestandes kann die in der Handreichung zum „Stand der Technik" des Bundesverbands IT-Sicherheit e. V. (TeleTrusT) vorgelegte Methode[59] herangezogen werden. Sodann lässt das „Berücksichtigen" die Prüfung zu, ob und inwieweit subjektive Gründe vorliegen, den Stand der Technik im konkreten Fall planmäßig zu unterschreiten.[60] An dieser Stelle wird sich bei der Umsetzung der Geschäftsmodelle entscheiden, in welchem Umfang aufgrund der DSGVO in IT-Sicherheit investiert werden muss, oder eine Investition zwar sinnvoll, aber freiwillig und somit beispielsweise später oder anders umgesetzt werden kann. So sieht Art. 32 DSGVO explizit vor, dass bei der Umsetzung technischer Maßnahmen auch die Implementierungskosten ins Verhältnis gesetzt werden dürfen. Dies führt zu einer wirtschaftlichen Verhältnismäßigkeitsprüfung, im Rahmen derer das Verletzungsrisiko beachtet werden kann. Das Gesetz gibt zwar keine Anhaltspunkte für die zulässige Einbeziehung wirtschaftlicher Faktoren vor, dies erweitert aber einstweilen eher den Argumentationsspielraum, als ihn zu verengen. Hier kann z. B. mittels IT-Sicherheits-Budgets oder umsatzbezogenen Investitionsquoten argumentiert werden.

Da der Tatbestand des Art. 32 DSGVO eine Bewertung und Steuerung von technischen, organisatorischen und rechtlichen Aspekten voraussetzt, wird eine Erfüllung dieser Norm in der Praxis nur hinreichend rechtssicher erfolgen können, wenn hierzu eine Expertise aus den Bereichen IT, IT-Sicherheit und IT-Recht zusammenkommt. Dies zu initiieren ist Aufgabe der Geschäftsleitung.

Um den Nachweis der getroffenen Maßnahmen zu gewährleisten, als auch den Grad des Berücksichtigens darlegen zu können, ist eine entsprechende Dokumentation der technischen und organisatorischen Maßnahmen erforderlich (Art. 5 Abs. 2 i. V. m. Abs. 1 lit. f DSGVO). Dazu sollte die konkreten Maßnahmen gemäß dem Stand der Technik ausgeführt werden und in Bereichen, in denen dieser Technologiestand nicht erreicht wird, die alternativ eingesetzten Maßnahmen genannt und begründet werden. Dadurch kann eine Berücksichtigung belegt und ein Bußgeld vermieden werden. Für die Zulässigkeit des Unterschreitens des Stands der Technik haftet der Verantwortliche bzw. der Auftragsverarbeiter.

Abbildung zur Dokumentation von technischen und organisatorischen Maßnahmen:

Maßnahmen	Beschreibung	Schutzbedarf	Stand der Technik		Wirksamkeitsprüfung
			objektiv-technisch	subjektive Auswahl	

58 Bartels/Backer; ITSiG-konforme Telemedien – Technische und organisatorische Vorkehrungen nach § 13 Abs. 7 Telemediengesetz, DuD – Datenschutz und Datensicherheit, 1/2016, 22-28, 27.
59 Bartels/Lawicki u. a., Handreichung zum „Stand der Technik" technischer und organisatorischer Maßnahmen, 2020-02, S. 11 ff.
60 Bartels/Backer, Die Berücksichtigung des Stands der Technik in der DSGVO, DuD 4-2018, 214.

Eine nicht dem Art. 32 DSGVO entsprechende Umsetzung von technischen und organisatorischen Maßnahmen kann die zuständige Datenschutzaufsichtsbehörde mit Bußgeldern ahnden. Gemäß Art. 83 Abs. 4 lit. a i. V. m. Art. 32 DSGVO können für die mangelnde Umsetzung Bußgelder von bis zu EUR 10.000.000 oder von bis zu 2 % des weltweit erzielten Vorjahresumsatzes verhängt werden, je nachdem, welcher der Beträge höher ist. Beachtlich ist, dass unabhängig von der Umsetzung der technischen und organisatorischen Maßnahmen selbst, auch Bußgelder allein für die fehlende oder mangelhafte Dokumentation[61] verfügt werden können, deren Bußgeldrahmen zweifach so hoch ist wie der vorgenannte, Art. 83 Abs. 5 lit. e i. V. m. Art. 5 Abs. 2 i. V. m. Abs. 1 lit. f DSGVO.

Eine weitere Herausforderung für die Beteiligten von kollaborativen Geschäftsmodellen wird die vertragliche Verpflichtung der jeweiligen Vertragsparteien auf Implementierung und Aufrechterhaltung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO sein. Eine Verpflichtung etwa einer Vertragspartei auf Maßnahmen, die vollumfänglich dem Stand der Technik zu entsprechen haben, wäre aus Sicht der DSGVO grundsätzlich überobligatorisch, würde unnötig kostensteigernd wirken und legte die Gefahr bereits anfänglich an, dass diese Verpflichtung wohl nicht eingehalten werden wird. Hier sind also differenzierte, am konkreten Einzelfall und seinem datenschutzrechtlich bestimmten Risiko ausgerichtete Verpflichtungen zu finden, die auch dokumentations- und prüffähig sind. Dies wird für kollaborative Plattformen insbesondere dort eine Herausforderung werden, wo Einzelunternehmer (z. B. Urheber, Know-how-Träger) in die Datenverarbeitung eingebunden werden. Da dieser ggf. nicht über hinreichende Ressourcen zur Schaffung der gesetzlichen IT-Sicherheit haben, ist zu prüfen, inwieweit hier allseits akzeptable Mindeststandards definiert werden können oder die Datenverarbeitung weitgehend auf die IT-Infrastruktur der Plattform verlagert werden kann, soweit dies nicht ohnehin geplant ist. Die Verletzung vertraglicher Pflichten auf bestimmte IT-Sicherheitsmaßnahmen können zu Schadensersatzforderungen führen, z. B. im Verhältnis Anbieter – Kunde oder Anbieter – Zulieferer (siehe oben).

Im Blick behalten sollten die Beteiligten von kollaborativen Geschäftsmodellen die Entwicklung der datenschutzspezifischen Zertifizierungsverfahren, der Datenschutzsiegel und -prüfzeichen für Dienstleistungen und Produkte nach Art. 42 DSGVO. Derartige Zertifizierungen werden sowohl den Anbietern als auch den Anwendern und auch den Intermediären (wie Plattformbetreibern) ein effizientes Mittel sein, um die Rechtssicherheit in Sachen Datenschutz zu erhöhen, die Vertragspartnerwahl zu vereinfachen und die dauerhafte Vertragstreue allseits besser nachzeichnen zu können. Derzeit fehlt es in Deutschland noch an den für eine Zertifizierung notwendigen Voraussetzungen, nämlich den Akkreditierungen der Zertifizierungsstellen. Diese ersten Akkreditierungen nach Art. 43 DSGVO sollen dieses Jahr erfolgen.[62]

Bereits im Rahmen der Planung und Modellierung der Geschäftsmodelle sollte der Datenschutz möglichst weitgehend strukturell angelegt sein. Die DSGVO verpflichtet nach Art. 25 DSGVO auch zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.[63] Zu beachten ist: Die gesetzlichen Pflichten aus Art. 25 DSGVO adressieren nicht den Hersteller eines Produktes oder den Anbieter einer Dienstleistung. Verpflichtet wird ausschließlich der Verantwortliche. Inhalt der Verpflichtung ist die Festlegung von technischen und organisatorischen Maßnahmen, „die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen“.[64] Bezugspunkte dabei sind die bereits in Art. 32 Abs. 1 DSGVO bestimmten Abwägungsaspekte. Weder aufsichtsbehördlich noch rechtswissenschaftlich ergibt sich bislang ein klares Bild, wie diese Anforderungen exakt umzusetzen sind. Die Beteiligten sollten somit auch diesen Anforderungsbereich und seine rechtlichen Entwicklungen beobachten.

61 Die Dokumentation dient dem nach Art. 5 Abs. 2 DSGVO erforderlichen Nachweis der Einhaltung der Verarbeitungsgrundsätze (Rechenschaftspflicht).
62 28. Tätigkeitsbericht zum Datenschutz des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit 2019, S. 71.
63 Diskutiert zumeist unter den englischen Begriffen „Data Protection by Design and by Default“.

3.3.2 Kollaborative Verarbeitung von Daten mit Personenbezug

Strukturmerkmal unserer beispielhaften Geschäftsmodelle ist die gemeinsame oder zumindest arbeitsteilige Datenverarbeitung. Dies betrifft vermittelnd auftretende Plattformen dadurch, dass Daten von mehreren potenziellen Vertragsparteien zusammengeführt werden. Plattformen aus dem Cluster Logistik akkumulieren ggf. Daten, um sie teilweise oder ganz durch einige oder sämtliche Beteiligte auszuwerten. Die Plattformen, die im Kapitel 1 für die Bereiche Robotik und Engineering beschrieben sind, beraten Kunden oder erbringen diesen gegenüber Integrationsleistungen, die vor allem datenbasiert funktionieren. Soweit die dabei verarbeiteten Daten tatsächlich keinerlei Personenbezug aufweisen, findet die DSGVO keine Anwendung. Ungeachtet fehlender gesetzlicher Verpflichtungen sollte auch einer kollaborativen Verarbeitung von Daten ohne Personenbezug eine Vereinbarung zur IT-Sicherheit und ggf. zur Geheimhaltung unterlegt werden.

Ein Personenbezug liegt nach Art. 4 Ziff. 1 DSGVO vor bei „alle(n) Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (…) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.“

Inwieweit Daten mit Personenbezug verarbeitet werden, ist im Rahmen der Geschäftsmodell-Entwicklung möglichst frühzeitig und exakt zu bestimmen. Zur Verdeutlichung der praktischen Feststellungsschwierigkeiten kann ein beispielhafter Anwendungsfall aus dem Bereich Logistik dienen: Die Messwerte von Sensoren, die den Aufenthaltsort eines Containers abbilden, weisen in der Regel allein keinen Personenbezug auf. Soweit nun zeitgleiche Informationen über konkrete Fahrerinnen oder Fahrer vorliegen, ergeben sich Daten mit Personenbezug (Aufenthaltsort und -zeiten, Route etc.) für diejenigen, die diese Daten zusammenführen oder zusammenführen könnten. Soweit feststeht, dass Daten mit Personenbezug kollaborativ verarbeitet werden, sind die drei oben genannten Modelle zu prüfen: die Auftragsverarbeitung (Art. 28 DSGVO), die gemeinsame Verantwortlichkeit (Art. 26 DSGVO) oder die getrennte Verantwortlichkeit (Art. 5 Abs. 1 1. TS; 24 Abs. 1 DSGVO).

64 Art. 25 Abs. 1 a. E. DSGVO.

Eine Auftragsverarbeitung setzt positiv voraus, dass ein Auftragsverarbeiter für einen Auftraggeber Daten mit Personenbezug verarbeitet. Verantwortlicher ist hier also der Auftraggeber. Negative Voraussetzung einer Auftragsverarbeitung ist zugleich der Ausschluss einer eigenen Verantwortlichkeit des Auftragnehmers bei einer Verarbeitung für den Auftraggeber. Verantwortlich im Sinne der DSGVO ist nach Art. 4 Ziff. 7, wer allein oder gemeinsam mit anderen über Mittel und Zwecke der Verarbeitung entscheidet. Verkürzt dargestellt bedeutet das: Verarbeitet ein Beteiligter des Geschäftsmodells die personenbezogenen Daten eines Dritten auf dessen Auftrag zu dessen Zwecken, liegt in der Regel eine Auftragsverarbeitung vor. Ebenso verkürzt: werden „fremde Daten" zu eigenen Zwecken oder „eigene Daten" zu fremden Zwecken verarbeitet, kann nur eine gemeinsame oder getrennte Verantwortlichkeit, aber keine Auftragsverarbeitung vorliegen.

Eine gemeinsame Verantwortlichkeit liegt gemäß Art. 26 DSGVO vor, wenn zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen. Sämtliche Verantwortliche benötigen für die Verarbeitung eine eigene Rechtsgrundlage nach Art. 6 DSGVO. Von einer getrennten Verantwortlichkeit im Rahmen einer kollaborativen Verarbeitung ist schließlich auszugehen, wenn zwar mehrere Verantwortliche an der Verarbeitung von Daten mit Personenbezug beteiligt sind, dazu aber keine Einigung über die Zwecke und Mittel der Verarbeitung treffen (sondern z. B. nur über eine der beiden Aspekte).

Art. 26 Abs. S. 2 und 28 Abs. 3 DSGVO fordern jeweils den Abschluss einer datenschutzrechtlichen Vereinbarung über die Verarbeitung, einmal eine sogenannte JC-Vereinbarung (Joint-Controllership-Vereinbarung), einmal eine AV-Vereinbarung (Auftragsverarbeitungs-Vereinbarung).[65] In beiden Vereinbarungen sind diejenigen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO zu beschreiben (siehe oben), die bezogen auf die im Leistungsvertrag vereinbarten Leistungen relevant sind. Bei einer getrennten Verantwortlichkeit ist eine vergleichbare Vereinbarung gesetzlich nicht vorgeschrieben. Ob eine solche im Einzelfall vorteilhaft ist, kann nur anhand der konkreten Interessen geprüft werden. Es wäre jedenfalls darauf zu achten, dass durch eine solche Vereinbarung nicht die Voraussetzungen von Art. 26 oder 28 DSGVO geschaffen werden, die es ggf. zu vermeiden galt.

3.3.3 Telemediengesetz

Durch das erste IT-Sicherheitsgesetz wurde 2015 das Telemediengesetz (TMG) geändert. In dem neu eingefügten Absatz 7 des § 13 TMG wurde normiert, dass Telemediendienstanbieter ihre technischen Einrichtungen durch technische und organisatorische Vorkehrungen zu schützen haben. Bei der Auswahl und Unterhaltung dieser Maßnahmen muss wiederum der Stand der Technik berücksichtigt werden. Die gesetzliche Pflicht knüpft auch, aber nicht nur an den Schutz von Daten mit Personenbezug an. Sie adressiert alle geschäftsmäßig angebotenen Telemedien (§ 13 Abs. 7 S. 1 i. V. m. § 2 Ziff. 1 TMG). Darunter fallen auch Websites, Online-Plattformen, online erbrachte Dienste, Software-as-a-Service, wie sie im Rahmen kollaborativer Geschäftsmodelle aufgebaut werden.

Bei der Auswahl und Aufrechterhaltung dieser Maßnahmen ist ebenfalls der Stand der Technik zu berücksichtigen. Das setzt eine (gesetzlich ungeschriebene) Schutzbedarfsanalyse und die oben dargestellte zweistufige Prüfung vom objektiven Technologiestand und den subjektiven Umsetzungserfordernissen voraus.[66]

65 Die inhaltlichen Anforderungen einer JC-Vereinbarung sind in Art. 26 Abs. 1 und 2 nur punktuell angegeben, die einer AV-Vereinbarung ergeben sich detailliert aus Art. 28 Abs. 3 DSGVO.
66 Vgl. Bartels/Backer, ITSiG-konforme Telemedien – Technische und organisatorische Vorkehrungen nach § 13 Abs. 7 Telemediengesetz, DuD 1/2016, S. 22.

Die Verletzung der Sicherheitsanforderungen der Norm kann nach § 16 Abs. 2 Ziff. 3, Abs. 3 TMG zwar (teilweise) mit Bußgeldern von bis zu EUR 50.000 geahndet werden. Praktische Fälle sind dazu allerdings nicht bekannt. Das mag daran liegen, dass bereits unklar ist, welche Behörde für die Ahndung von Verstößen zuständig ist, die Landesmedienanstalten oder die Datenschutzaufsichtsbehörden der Länder.[67]

Die Beteiligten betreffender kollaborativer Geschäftsmodelle sollten diese Norm dennoch im Blick behalten. Das die Norm einführende IT-Sicherheitsgesetz, welches in seiner 2017 geänderten Fassung der Umsetzung der EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS-Richtlinie)[68] dient, steht vor einer erneuten und sehr grundlegenden Änderung, was unten ausgeführt wird.

3.3.4 IT-Sicherheitsgesetz 2.0

Die folgenden Ausführungen beruhen auf dem Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat (BMI) „Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0 – IT-SiG 2.0)" mit Bearbeitungsstand vom 07.05.2020 (nachfolgend „Ref-ENT"). Es ist zu erwarten, dass der Entwurf noch erheblichen Änderungen unterliegt, bevor er ggf. vom Bundestag als Gesetz verabschiedet werden wird.

Das geltende IT-Sicherheitsgesetz adressiert vorrangig die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber) gemäß § 2 Ziff. 10 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI).[69] Der Ref-ENT erweitert die KRITIS-Sektoren hier lediglich um den der Entsorgung. Neben die Hauptadressaten treten die o. g. Telemediendienstanbieter sowie die Anbieter digitaler Dienste[70]. Digitale Dienste im Sinne des BSI sind die Online-Marktplätze, Online-Suchmaschinen und Cloud-Computing-Dienste, die den Anforderungen des § 2 Abs. 11 BSI entsprechen. Die Pflichten des BSI gelten für die Anbieter digitaler Dienste jedoch nur, soweit sie nicht weniger als 50 Personen beschäftigen und ihr Jahresumsatz bzw. die Jahresbilanz EUR 10 Mio. nicht übersteigt.[71] Greift diese Ausnahme für Kleinstunternehmen und kleine Unternehmen nicht, sind unter anderem besondere Meldepflichten[72] gegenüber dem BSI bei IT-Sicherheitsvorfällen zu erfüllen und IT-Sicherheitsmaßnahmen nach den Maßgaben des §8c Abs. 2 BSI umsetzen. Auch hier ist der Stand der Technik zu berücksichtigen.

Eine wesentliche Erweiterung des Kreises der Verpflichteten ergibt sich aus der Schaffung der Kategorie von Unternehmen im besonderen öffentlichen Interesse (nachfolgend „Unternehmen i. b. ö. I."), § 2 Abs. 14 Ref-ENT. Neben Rüstungs-, Raumfahrt- und IT-Sicherheitsunternehmen[73] und Chemieunternehmen sind hier auch Unternehmen die aufgrund ihrer volkswirtschaftlichen Bedeutung und insbesondere ihrer erbrachten Wertschöpfung von besonderem öffentlichem Interesse sind (nachfolgend „Unternehmen i. b. ö. I."), um-

67 Vgl. Bartels/Backer, ITSiG-konforme Telemedien – Technische und organisatorische Vorkehrungen nach § 13 Abs. 7 Telemediengesetz, DuD 1/2016, S. 22 f.
68 Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.
69 Auf eine Darstellung der branchenspezifischen Normen u. a. des Telekommunikationsgesetzes (TKG), des Atomgesetzes und des Gesetzes über die Elektrizitäts- und Gasversorgung (EnWG), die durch das IT-Sicherheitsgesetz geschaffen oder geändert wurden, wird hier verzichtet.
70 § 8c Abs. 1 i. V. m. § 2 Abs. 12 BSIG.
71 § 8d Abs. 4 BSIG.
72 Vgl. https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/DigitaleDienste/Meldungen/meldungen_node.html [14.07.2020]
73 S. Verweis auf die Definitionen in der Außenwirtschaftsverordnung.

fasst. Eine nähere Bestimmung der Unternehmen wird durch Rechtsverordnung erfolgen (§ 10 Abs. 5 Ref-ENT), wie dies hinsichtlich der KRITIS-Betreiber derzeit bereits der Fall ist (§ 10 Abs. 1 BSIG). Die Unternehmen i. b. ö. l. haben dem BSI ein IT-Sicherheitskonzept vorzulegen (§ 8f Abs. 1 Ref-ENT). Die Möglichkeit, die Umsetzung der Anforderungen an die IT-Sicherheit mittels Nutzung eines Branchenmindeststandards nachzuweisen, sollen die Unternehmen i. b. ö. l. allerdings nicht erhalten.

Nicht minder relevant ist die Einführung und Neudefinition sogenannter Kernkomponenten für Kritische Infrastrukturen („KRITIS-Kernkomponenten"), § 9b Abs. 13 Ref-ENT. KRITIS-Kernkomponenten sind danach IT-Produkte, die in Kritischen Infrastrukturen eingesetzt werden und die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit dieser IT-Produkte zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit Kritischer Infrastrukturen oder zu Gefährdungen für die öffentliche Sicherheit führen können. Ob und inwieweit die Beteiligten kollaborativer Geschäftsmodelle direkt oder mittelbar zu den (neuen) Adressaten des Gesetzes zählen können, ist zu prüfen. Jedenfalls lässt sich prognostizieren, dass die Ausweitung des Anwendungsbereichs des IT-Sicherheitsgesetzes auch außerhalb der gesetzlichen Adressaten dazu führen wird, dass zwischen Vertragsparteien die subjektiven Erwartungshaltungen hinsichtlich vertraglich zu vereinbarender und vereinbarter IT-Sicherheit steigen wird. Gleiches gilt für gerichtlich angelegte Prüfungsmaßstäbe.

Der Begriff der „Cyberkritikalität" aus § 8g des Referentenentwurfs aus 02/2019 findet sich im vorbezeichneten Ref-ENT nicht mehr. Allerdings regelt nunmehr § 9b Abs. 3 Ref-ENT, dass das Bundesministerium des Innern, für Bau und Heimat zum Zwecke der Gewährleistung der nationalen Sicherheitsinteressen der Bundesrepublik Deutschland den Einsatz von kritischen Komponenten in Hinblick auf die Vertrauenswürdigkeit des Herstellers prüfen kann und gegenüber dem Betreiber der Kritischen Infrastruktur den Einsatz untersagen darf, wenn der Hersteller der kritischen Komponente nicht vertrauenswürdig ist. Ein Hersteller ist insbesondere nicht vertrauenswürdig, wenn er gegen die in einer Garantieerklärung nach Abs. 2 eingegangen Verpflichtungen und Versicherungen verstoßen hat oder dort angegebene Tatsachen unwahr sind[74], Sicherheitsprüfungen nicht angemessen unterstützt, bekannte Schwachstellen nicht unverzüglich dem Betreiber Kritischer Infrastrukturen meldet und nicht beseitigt[75] sowie hinsichtlich etwaig vorhandener technischer Eigenschaften, die eine missbräuchliche Einwirkung auf die IT-Sicherheit ermöglichen, nachweist, dass er die Eigenschaften implementiert bzw. beseitigt hat[76].

Hintergrund ist, dass künftig nach § 9b Abs. 2 Ref-ENT sogenannte Kritische Komponenten (im Sinne von Abs. 1) nur noch von solchen Herstellern eingesetzt werden dürfen, die eine Garantieerklärung über ihre Vertrauenswürdigkeit gegenüber dem Betreiber der Kritischen Infrastruktur abgeben. Diese Erklärung muss die gesamte Lieferkette des Herstellers umfassen. Das Bundesministerium des Innern, für Bau und Heimat soll dazu Mindestanforderungen für die Garantieerklärung durch Allgemeinverfügung festlegen. Die Garantieerklärung muss erläutern, ob und wie der Hersteller sicherstellt, dass die kritische Komponente über keine technischen Eigenschaften verfügt, die geeignet sind, missbräuchlich auf die

74 § 9b Abs. 4 Ziff. 1 und 2 Ref-ENT.
75 § 9b Abs. 4 Ziff. 3 und 4 Ref-ENT.
76 § 9b Abs. 4 Ziff. 5 Ref-ENT.

Sicherheit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur (etwa Sabotage, Spionage oder Terrorismus) einwirken zu können.

Wie auch im Vorentwurf ist die Einführung eines freiwilligen IT-Sicherheitskennzeichen (§9a IT-Sicherheitsgesetz Ref-ENT) für Hersteller zur Darstellung des Vorliegens bestimmter IT-Sicherheitseigenschaften seines Produktes geplant. Das IT-Sicherheitskennzeichen soll insbesondere Verbraucherinnen und Verbraucher in die Lage versetzen, sich im Rahmen der Kaufentscheidung ein Urteil zu darüber zu verschaffen, inwieweit das jeweilige IT-Produkt bzw. dessen Hersteller aktuelle Sicherheitsstandards in ausreichender Form berücksichtigt. Der Antrag zur Nutzung des Kennzeichens ist beim BSI zu stellen. In welchem Verhältnis dieses IT-Sicherheitskennzeichen zu dem im Cybersecurity Act der EU[77] angelegten Cybersicherheitszertifikat stehen soll, ist nach wie vor unklar.

3.4 IP und Know-how-Schutz

Im Rahmen von kollaborativen Geschäftsmodellen werden häufig auch immaterielle Geschäftswerte in die Zusammenarbeit eingebracht oder gehen aus dieser hervor. Unternehmen haben dabei das Interesse, ihr Know-how zu schützen und – im Falle einer Weitergabe – eine bestimmungsgemäße Verwendung sicherzustellen. Aus den Regelungen des Urheber- und Designrechts ergeben sich Ansatzpunkte zum Schutz von Unternehmensinformationen. Darüber hinaus können sich aus dem Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) weitere Konsequenzen für den Umgang mit sensiblen Unternehmensinformationen ergeben.

3.4.1 Urheber- und Designrecht

Immaterielle Geschäftswerte können zunächst durch das Urhebergesetz (UrhG) geschützt sein. Als geschützte Werkformen nennt § 2 UrhG etwa Darstellungen wissenschaftlicher und technischer Art (Nr. 7 UrhG), worunter z. B. Entwurfsskizzen von technischen Bauteilen oder Konstruktionspläne fallen können. Auch Computerprogramme (als Sprachwerke nach § 2 Abs. 1 Nr. 1 UrhG) und Datenbanken (§ 4 Abs. 2 UrhG) werden durch das UrhG erfasst. Die Zugehörigkeit zu diesen Werkkategorien begründet aus sich heraus jedoch noch keinen Urheberrechtsschutz. Erforderlich ist eine persönliche geistige Schöpfung (§ 2 Abs. 2 UrhG). Hierfür ist ein kreativer Schaffensprozess notwendig, der dem Erzeugnis etwas Neues und Eigentümliches verleiht. Nicht schutzfähig sind hingegen reine Ideen, die etwa einem Computerprogramm zu Grunde liegen (z. B. Algorithmen).

Das UrhG enthält zusätzlich Vorschriften zum Schutz von bestimmten Leistungen. Diese sogenannten Leistungsschutzrechte stehen dem Urheberrecht nahe, knüpfen aber nicht an das Vorliegen einer persönlichen geistigen Schöpfung an. Geschützt wird vielmehr der wirtschaftliche, organisatorische und technische Aufwand, der mit der Herstellung des jeweiligen Erzeugnisses einhergeht. In kollaborativen Wertschöpfungsnetzen ist in diesem Zusammenhang der Schutz von Datenbanken von Bedeutung. Denn Aufbau und Pflege einer Datenbank können mit erheblichem Aufwand verbunden sein. Mit § 87a UrhG besteht ein entsprechendes Leistungsschutzrecht für Datenbankhersteller. Die Vorschrift setzt u. a. voraus, dass die Beschaffung, Überprüfung oder Darstellung von Daten mit einer wesentlichen Investition verbunden ist. Als Datenbankhersteller gilt, wer diese Investition vorgenommen hat.

77 Verordnung des Europäischen Parlaments und des Rates über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) NR.526/2013 (Rechtsakt zur Cybersicherheit).

Neben dem urheberrechtlichen Werkschutz können Entwürfe, Modelle von Bauteilen, aber auch physischen Bauteile selbst (z. B. als Ergebnis von additiven Fertigungsmethoden), nach dem Designgesetz (DesignG) geschützt sein. Urheber- und Designschutz schließen einander nicht aus, sondern können nebeneinander bestehen. Für die Entstehung des Designschutzes ist eine Registereintragung erforderlich (§ 27 Abs. 1 DesignG). Die entsprechende Anmeldung zur Eintragung erfolgt beim Deutschen Patent- und Markenamt. Möglich ist aber auch die Eintragung in ein internationales Register. Voraussetzung für den Designschutz ist, dass das Design neu ist und Eigenart aufweist. Für die Neuheit eines Designs ist notwendig, dass vor dem Anmeldetag nicht bereits ein identisches Design offenbart worden ist (§ 2 DesignG). Ein Design weist Eigenart auf, wenn es sich von anderen bereits eingetragenen Designs unterscheidet (§ 2 Abs. 3 S. 1 DesignG).

Der Urheber hat das ausschließliche Recht zur Verwertung seines Werks (§ 15 Abs. 1 UrhG). Als Verwertungshandlungen kennt das UrhG u.a. das Recht auf Vervielfältigung, Verbreitung oder öffentliche Wiedergabe. Im Rahmen von kollaborativen Geschäftsmodellen dürfen geschützte Erzeugnisse, wie Baupläne, Computerprogramme oder Datenbanken nur mit Zustimmung des jeweiligen Rechtsinhabers auf Plattformen eingestellt und Dritten zur Verfügung gestellt werden. In derartigen Konstellationen sollte die Überlassung mit einer entsprechenden Nutzungsrechteeinräumung flankiert werden. Umgekehrt kann in bestimmten Konstellationen eine Klarstellung dahingehend erfolgen, dass der Vertragspartei die Nutzung für einen bestimmten Zweck gewährt wird (z. B. zur Anfertigung eines Bauteils im 3D-Druckverfahren), weitergehende Rechte aber ausdrücklich nicht eingeräumt werden.

Das eingetragene Design gewährt seinem Rechtsinhaber das ausschließliche Recht der Benutzung. Dritten gegenüber kann die Benutzung untersagt werden (§ 38 Abs. 1 DesignG). Als Benutzungshandlungen werden u.a. die Herstellung, das Anbieten und das Inverkehrbringen eines Erzeugnisses genannt. Die Benutzungsbeschränkungen können insbesondere im Bereich des 3D-Drucks von Bedeutung sein. So kann die Anfertigung, aber auch der Vertrieb von Bauteilen in das ausschließliche Benutzungsrecht der Designinhaberin oder des Designinhabers eingreifen.

Kommt es zu rechtswidrigen Verwertungshandlungen stehen dem geschädigten Unternehmen sowohl nach dem UrhG als auch dem DesignG verschiedene Ansprüche zu. Das UrhG gewährt dem Verletzten u. a. Ansprüche auf Beseitigung und Unterlassung, bei einer vorsätzlichen oder fahrlässigen Verletzungshandlung auch Ansprüche auf Schadensersatz (§ 97 Abs. 1, Abs. 2 UrhG). Gleiches gilt für die rechtswidrige Benutzung eines geschützten Designs (§ 42 Abs. 1, Abs. 2 UrhG). Rechtswidrig hergestellte Vervielfältigungsstücke, die etwa im Rahmen von 3D-Druckverfahren entstehen, können darüber hinaus Ansprüche auf Vernichtung, Rückruf und Überlassung begründen (§ 98 UrhG, § 43 DesignG).

3.4.2 Geschäftsgeheimnisschutzgesetz

Das Geschäftsgeheimnisschutzgesetz (GeschGehG)[78] spielt für die kollaborativen Geschäftsmodelle eine zentrale Rolle. Denn zum einen können in den Anwendungsbereich des GeschGehG mannigfaltige Informationen bzw. Leistungen, die nicht bereits durch bereichsspezifische Gesetze – wie das Urheberrechtsgesetz oder Designgesetz geschützt sind – fallen. Zum anderen gewährt das GeschGehG dem geschädigten Unternehmen diverse Ansprüche gegen den Täter: So hat der Inhaber eines Geschäftsgeheimnisses gegenüber demjenigen, der sein Geschäftsgeheimnis unbefugt erwirbt, nutzt oder offenlegt Anspruch auf Beseitigung und Unterlassung (§ 6 GeschGehG), Vernichtung, Herausgabe, Rückruf, Entfernung und Rücknahme vom Markt (§ 7), Auskunft über rechtsverletzende Produkte, Schadensersatz bei Verletzung der Auskunftspflicht (§ 8) und Schadenersatz (§ 10).[79]

Voraussetzung für mögliche Ansprüche ist das Vorliegen eines Geschäftsgeheimnisses im Sinne von § 2 Ziff. 1 GeschGehG: Verkürzt formuliert ist ein Geschäftsgeheimnis eine Information, die a) geheim ist und daher von wirtschaftlichem Wert ist, b) durch angemessene Geheimhaltungsmaßnahmen des rechtmäßigen Inhabers des Geheimnisses geschützt wird und c) bei der ein berechtigtes Interesse an der Geheimhaltung besteht.

Als Geschäftsgeheimnisse können somit Informationen z. B. über die Produktentwicklung (Zeichnungen, Eigenschaften von Komponenten, Zusammensetzungen, Konstruktionen), Herstellung (Anforderungen, Spezifikationen, Fertigungs- und Testverfahren, Vorgehensmodelle, Kapazitäten, Kostenstrukturen), Einkauf/Vertrieb (Bezugsquellen, Lieferanten, Konditionen, Kalkulationsgrundlagen, Vertriebswege, Logistikinformationen), Marketing (Kundendaten, Kundenverhalten/-wünsche, Marktanalysen), Unternehmensentwicklung/-strategie und Transaktionen (Geschäftsmodelle, Business-Pläne, Investitions- und Expansionspläne, Marktentwicklung, Informationen über M&A-Verhandlungen) und auch Informationstechnik (IT-Architektur, Eigenentwicklungen, Sourcecode, Algorithmen, Inhalts- und Meta-Daten, Datenanalysen) geschützt sein.

Während die o. g. Voraussetzungen zu a) und c) in der Regel einfach festzustellen sind, ergeben sich erhebliche Herausforderungen hinsichtlich der angemessenen Geheimhaltungsmaßnahmen. Zu den Geheimhaltungsmaßnahmen zählen technische, organisatorische und rechtliche Maßnahmen. Zum erforderlichen Niveau der Maßnahmen trifft das Gesetz keine Maßgaben. Als Faustformel darf einstweilen unterstellt werden, dass zumindest für Geheimnisse, die ein hohes bis sehr hohes Risiko bedingen, Maßnahmen nur dann angemessen sind, wenn sie den Stand der Technik hinreichend berücksichtigen (siehe oben). Die Umsetzung der Geheimhaltungsmaßnahmen sollte in enger Abstimmung mit der Umsetzung der Informationssicherheitsmaßnahmen nach Art. 32 DSGVO (siehe oben) erfolgen, da hier die Schnittmenge der Maßnahmen und mit der Umsetzung befassten Personen (IT, IT-Sicherheit, Datenschutzbeauftragter, Compliance) sehr groß ist.

78 Das deutsche Geschäftsgeheimnisschutzgesetz setzt die sogenannte EU-Know-how-Richtlinie (EU 2016/943) in nationales Recht um.

79 Ausnahmen im Sinne ausdrücklich erlaubter oder auch gerechtfertigter Handlungen sieht das Gesetz in §§ 3 und 5 GeschGehG vor (z. B. vor für ein zulässiges Reverse Engineering oder sogenanntes Whistle Blowing).

Zu den rechtlichen Maßnahmen gehören insbesondere einseitige Verschwiegenheitsverpflichtungserklärungen (NDA, Non Disclosure Agreement) und zwei- bzw. mehrseitige Verträge, die Regelungen im Sinne des GeschGehG enthalten sollten, wie z. B. Forschungs- und Entwicklungs-, Kooperations- und (Software-)Lizenzverträge (siehe Vorgehensweise zur Umsetzung des GeschGehG).

Vorgehensweise zur Umsetzung des GeschGehG

- Geschäftsgeheimnisse identifizieren und klassifizieren
- Schutzbedarfsanalyse: Risiken ermitteln
- Angemessene Geheimhaltungsmaßnahmen ermitteln: Technische, organisatorische und rechtliche Maßnahmen bestimmen anhand des Schutzbedarfs
- Dokumentation und Schutzkonzept: Umsetzung der Maßnahmen in der Unternehmenspraxis feststellen und planen
- Revision: Mindestens jährliche Überprüfung des Geschäftsgeheimnis-Schutzkonzepts
- Organisation und Schulung im Unternehmen: Verfahren, Zuständigkeiten, Vorgaben, Ziele
- Monitoring Rechtsverletzungen: Beobachtung von Offenlegung, Nutzung und Erlangen durch Unbefugte
- Verträge schließen/anpassen:
  - Arbeitsverträge
  - Verträge mit freien Mitarbeitern
  - Subunternehmerverträge
  - Kooperationsverträge
  - Lizenzverträge
  - Forschungs- und Entwicklungsverträge
  - NDA

Für die Umsetzung des Gesetzes gibt es keine Aufsichtsbehörde. Es handelt sich um Verpflichtungen allein sich selbst gegenüber (Obliegenheiten). Wer also die Verletzung der Geheimnisse und die angemessenen Geheimhaltungsmaßnahmen nicht zivilprozessual darlegen und beweisen kann, wird gerichtlich unterliegen. Zu Beweiszwecken ist deshalb ein Geschäftsgeheimnisschutzkonzept zu erstellen und aktuell zu halten.

4 Zusammenfassung

Dieser Leitfaden fasst die wichtigsten Erkenntnisse aus der Fachgruppenarbeit zu kollaborativen Geschäftsmodellen und daraus resultierenden rechtlichen Fragestellungen der Begleitforschung des Technologieprogramms PAiCE zusammen. Dabei wird zunächst erläutert, was im Rahmen dieses Leitfadens unter kollaborativen Wertschöpfungssystemen und Geschäftsmodellen verstanden wird. Zur Veranschaulichung werden insgesamt vier verschiedene kollborative Wertschöpfungssysteme vorgestellt und kurz beschrieben.

Anschließend behandelt der Leitfaden zunächst die Thematik der Entwicklung kollaborativer Geschäftsmodelle. Hierfür wurden folgende Phasen der Geschäftsmodellentwicklung skizziert:

- Analyse des Ökosystems
- Ideengenerierung
- Bewertung & Ausgestaltung
- Verifizierung der Annahmen
- Prototyping
- Markteintritt

Für jede Phase werden zudem Tools und Methoden aufgeführt, die sich dabei zielführend einsetzen lassen. Im Anschluß wird die Visualisierung von Wertschöpfungssystemen erläutert. Dies umfasst sowohl die Wertschöpfungsprozesse innerhalb der zu betrachtenden Wertschöpfungseinheit (z. B. innerhalb einer Plattform) als auch die Beziehungen zwischen den beteiligten Akteursgruppen eines Wertschöpfungssystems. Darüber hinaus werden die größten Herausforderungen bei der Entwicklung kollaborativer Geschäftsmodelle herausgestellt. Dazu zählen:

- ein gemeinsames Verständnis zu entwickeln
- das Betriebsmodell zu erarbeiten sowie
- das Klären von Datenzugang und -nutzung

Der zweite Teil des Leitfadens widmet sich anschließend den rechtlichen Herausforderungen kollaborativer Geschäftmodelle. Dabei werden zunächst mögliche Arten von Verträgen und Vertragskonstellationen beleuchtet und aufgezeigt, inwiefern diese bereits frühzeitig bei der Entwicklung eines kollaborativen Geschäftsmodells auf ihre Passfähigkeit zu prüfen sind. Anschließend werden die Einbeziehung von allgemeinen Geschäftsbedingungen (AGB) sowie Fragen zur Haftung und zum Risikomanagement erläutert. Dabei wird u. a. auch auf die Verantwortung von Plattformbetreibenden nach dem Telemediengesetz eingegangen.

Des Weiteren behandelt der Leitfaden die Thematik der gesetzlichen oder obligatorischen Anforderungen an IT-Sicherheit und Datenschutz. Eine wesentliche Rolle spielt dabei insbesondere die Umsetzung geeigneter technischer und organisatorischer Maßnahmen unter Berücksichtigung des Stands der Technik und wie diese Maßnahmen zu dokumentieren sind. Weitere Schwerpunkte bilden die kollaborative Verarbeitung von Daten mit Personenbezug, das Telemediengesetz und das künftige IT-Sicherheitsgesetz 2.0. Es wird beschrieben, in welchen Konstellationen welche datenschutz-rechtlichen Vereinbarungen zwischen den Vertragsparteien zu schließen sind und wie sich die Modelle abgrenzen lassen. Abschließend wird der Know-how-Schutz thematisiert, wobei sowohl das Urheber- und Designrecht als auch das Geschäftsgeheimnisschutzgesetz behandelt werden.

Anhang

A1 Checkliste Geschäftsmodellentwicklung

- Wer sind die Kundinnen und Kunden?
  - Lassen sich diese in einzelne Segmente unterteilen?
- Wie lautet das Nutzenversprechen an die Zielgruppe?
  - Welche Bedürfnisse werden damit adressiert?
- Sind Kostenstruktur und Ertragsströme quantifiziert?
- Wie wird die Leistung für Kundinnen und Kunden erbracht?
  - Welche Prozesse und Aktivitäten stehen dabei im Mittelpunkt?
  - Welche Ressourcen sind dafür von Bedeutung?
- Welche weiteren Akteursgruppen sind für das Wertschöpfungssystem relevant?
  - Zwischen welchen Beteiligten werden Produkte und Dienstleistungen ausgetauscht?
  - Wo finden Zahlungsströme und Datenflüsse statt?
  - Bestehen Vereinbarungen bezüglich Datenzugang und -nutzung?
- Handelt es sich um ein Plattform-Geschäftsmodell?
  - Wer betreibt die Plattform?
- Welche Rollen übernehmen die beteiligten Akteursgruppen?
  - Welcher Mehrwert bietet sich den Beteiligten?
  - Gibt es eine gemeinsame Vision?

A2 Checkliste rechtliche Fragestellungen

Vertragsgestaltung

- Rollen und Verantwortlichkeiten im Wertschöpfungsnetz ermitteln
- Festlegung der vertraglichen Pflichten, die ein Akteur (allein oder in Kooperation mit anderen) übernimmt
- Verträge entlang der jeweiligen Pflichten gestalten (z. B. als Dienst-/Werkvertrag oder typengemischter Vertrag)
- Bei AGB die gesetzlichen Beschränkungen (etwa bezüglich Haftungsbeschränkungen oder Pauschalisierung von Schadensersatzansprüchen) beachten

Haftung

- Haftungsrisiken entlang der gesamten Wertschöpfungskette identifizieren
- Bei vertraglichen Haftungsbeschränkungen die (AGB-)rechtlichen Beschränkungen beachten

IT-Sicherheit und Datenschutz

- Frühzeitige Identifikation, ob und in welchem Umfang personenbezogen Daten verarbeitet werden
- Gewährleistung der Sicherheit der Datenverarbeitung durch technische und organisatorische Maßnahmen unter Berücksichtigung des Stands der Technik
- Nachweis der Umsetzung der getroffenen Maßnahmen durch eine entsprechende Dokumentation
- Feststellung der datenschutzrechtlichen Verantwortlichkeit unter den Beteiligten eines kollaborativen Wertschöpfungsnetzes
- Abschluss einer entsprechenden datenschutzrechtlichen Vereinbarung (Joint-Controllership-Vereinbarung oder Auftragsverarbeitungs-Vereinbarung)

IP und Know-how-Schutz

- Immaterielle Geschäftswerte identifizieren, die im Rahmen einer Kollaboration ausgetauscht oder weitergegeben werden sollen und die jeweilige Schutzfähigkeit nach dem UrhG und DesignG prüfen
- Immaterielle Geschäftswerte sollten nur mit entsprechender Nutzungsrechteeinräumung überlassen werden

Geschäftsgeheimnisschutz

- Identifikation der zu schützenden Geschäftsgeheimnisse und Risikozuordnung
- Umsetzung angemessener Geheimhaltungsmaßnahmen und deren Dokumentation (Geschäftsgeheimnis-Schutzkonzept)

www.paice.de