Die Lizenzierung von nicht-personenbezogenen Daten

Eine rechtliche und rechtsökonomische Analyse

Frank Rosenkranz und Marc Scheufen[*]

erschienen in: Zeitschrift für Digitalisierung und Recht (ZfDR), Jg. 2, Nr. 2 , S. 159-198

Mit Digitalisierung und der Vernetzung von Leistungen, Produkten, Kunden und Märkten werden Daten zu einer Schlüsselressource. Aus rechtlicher Perspektive rücken daher der Zugang zu Daten und die vertragliche Möglichkeit seiner Gewährung immer mehr in den Vordergrund. Erste Ansätze eines Datenvertragsrechts lassen sich bereits erkennen. Für die Lizenzierung nicht-personenbezogener Daten stehen unterschiedliche Vertragstypen zur Verfügung, Orientierung bieten zudem die bereits erprobten Know-How-Verträge.

Auch aus ökonomischer Perspektive ist der Zugang zu Daten entscheidend. Dieser bedingt nicht nur Dateninteroperabilität, sondern auch einheitliche, wenngleich sektorspezifische Standards. Neben den gesetzlichen Zugangsrechten haben individualvertragliche Ansätze besondere Bedeutung. Datenmusterverträge und Vertragsgeneratoren können dabei die Transaktionskosten senken.

Inhaltsübersicht

---

[*] Der Autor Rosenkranz ist Notarassessor bei der Rheinischen Notarkammer sowie Lehrbeauftragter an der Juristischen Fakultät der Ruhr-Universität Bochum und war vorher Juniorprofessor für Bürgerliches Recht im digitalen Zeitalter ebenda. Der Autor Scheufen ist Akademischer Rat auf Zeit ebenda und Economist in der Forschungsgruppe „Big Data Analytics“ am Institut der Wirtschaft, Köln. Dieser Beitrag entstand im Rahmen eines vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Forschungs- und Entwicklungsprojekt (Fördernummer: IEDS003). Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

I. Einleitung

Mit der zunehmenden Digitalisierung und damit einhergehend der Vernetzung von Leistungen, Produkten, Kunden und Märkten werden Daten in zweierlei Hinsicht zu

einer Schlüsselressource, die die wirtschaftliche Leistungsfähigkeit und den Wohlstand in der Datenökonomie sicherstellen.[1]

Zuerst sind alle digitalen Geschäftsmodelle notwendig in technischer Hinsicht datenbasiert. Digitale Informationstechnologie beruht auf der Verarbeitung von codierter, maschinenlesbarer Information[2]. Hierin unterscheiden sich auch originär digitale nicht von digitalisierten Geschäftsmodellen. Die Daten sind lediglich Schmiermittel, die ein reibungsloses Funktionieren der Maschinen sicherstellen.[3] Zweitens können Daten aber selbst der Rohstoff sein, der das Geschäftsmodell antreibt. Die datenabhängigen Leistungen können dabei eigenständig oder lediglich Ergänzungen zu anderen Dienstleistungen sein. Ihr wirtschaftlicher Wert beruht hier aber stets auf der Verarbeitung der inhaltlichen Ebene der Daten zu neuen Erkenntnissen. Dieser zweiten Variante zuzuordnen sind auch die Fälle, in denen Unternehmen die bei ihnen anfallenden Daten in Produktionsabläufen und Geschäftsprozessen einsetzen, um diese effizienter auszugestalten (z.B. Reduzierung der Produktionskosten, Vermeidung von Produktionsausfällen, uvm.).

Die besondere Eigenschaft, dass Daten nicht-rival im Konsum und damit nicht knapp sind, hebt die Besonderheit für die Bewirtschaftung von Daten im Allgemeinen und das Teilen dieser Daten im Besonderen hervor, um die wirtschaftlichen Potentiale aus Daten zu realisieren. Daten sind dabei sowohl Treiber als auch Befähiger neuer datengetriebener Geschäftsmodelle – das autonome Fahrzeug oder der intelligente Kühlschrank, der eigenständig unsere aufgebrauchten Lebensmittel nachbestellt, sind dabei längst schon keine Zukunftsutopien mehr.

Die Dynamik, mit der die Daten unsere Wirtschaft und Gesellschaft verändert, schafft neue und besondere Herausforderungen nicht nur aus technischer und wirtschaftlicher, sondern im besonderen Maße auch aus rechtlicher Perspektive. So ergeben sich im Datenzeitalter zunehmend Fragestellungen, die sich im analogen Entstehungskontexts der zivilrechtlichen Normen bisher nie stellten. Hier treffen historisch gewachsene Pfadabhängigkeiten auf neue digitale Besonderheiten, auf die durch die zur Entstehung neuer und Reformierung bestehender Rechtsordnungen zunehmend reagiert wird. So versucht der kürzlich von der EU-Kommission vorgeschlagene Data Act[4] auf diese Herausforderungen zu reagieren und besondere Fragestellungen der Datenökonomie mit Normen zu begleiten. Nichtsdestotrotz können auch bestehende, vermeintlich analoge Rechtsnormen des Zivilrechts bereits heute viele Fragestellungen und Besonderheiten digitaler (Plattform)ökonomien rechtssicher beantworten.

Die praktische Bedeutung der Daten steht immer noch im umgekehrten Verhältnis zu deren rechtlicher Aufarbeitung. Gerade die rechtlichen Probleme und Fragestellungen im Umgang mit nicht-personenbezogenen Industriedaten stehen noch am Anfang ihrer wissenschaftlichen Durchdringung. Die vorliegende Studie hat das Ziel, hierzu einen Beitrag zu leisten. Eine Besonderheit liegt zudem in der Verbindung mit

---

1 Siehe hierzu Aliu/Azkan/Bresser/Demary/Engels/Fiedler/Fritsch/Geelhaar/Goecke/Iggenna/Korte/Krotova/Lichtblau/Lis/Maisel/Müller/Otto/Rusche/Scheufen/Schmitz/Spiekermann/Thiele/Trautmann, Data Economy: Status Quo der deutschen Wirtschaft & Handlungsfelder in der Data Economy, Studie für das Bundesministerium für Wirtschaft und Energie (BMWi), 2019.

2 Vgl. zu diesem Verständnis z.B. *Zech,* Information als Schutzgegenstand, 2012, S. 32; *Zech*, CR 2015, 137, 138.

3 *Riehm,* VersR 2019, 714.

4 Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM(2022) 68 final.

rechtsökonomischen Untersuchungen, woraus unmittelbare Handlungsempfehlungen abgeleitet werden können.

Ausgangspunkt der Untersuchung ist eine Matrix der Datenbewirtschaftung, die Orientierung für praxisorientierte Anwendungen rechtlicher Fragestellungen im weiteren Verlauf sein soll (II.). Die anschließende rechtliche Analyse geht vom herkömmlichen Drei-Ebenen-Modell (III.1.) und dem Fehlen spezifischer eigentumsähnlicher Datenherrschaftsrechte (III.3.) aus. Auf dieser Basis werden die möglichen Regelungsgegenstände und Regelungsinhalte von Datennutzungsverträgen (III.4.) ausgearbeitet. Die rechtsökonomische Analyse widmet sich schließlich dem Datenzugang (IV.1.) und Datenmusterverträgen (IV.2.).

II. Arten der Bewirtschaftung von Daten

Die rechtlichen Problemstellungen bei der Bewirtschaftung von Daten müssen im Kontext der unterschiedlichen Arten und Anwendungsbeispiele der Datenbewirtschaftung gesehen werden. Eine Einordnung dieser Anwendungsbeispiele zur Beschreibung der Arten der Datenbewirtschaftung orientiert sich in diesem Zusammenhang an zwei zentralen Fragestellungen: (1) Woher kommen die Daten? Vor diesem Hintergrund ist bei der Datenherkunft zwischen intern, d.h. vom Unternehmen selbst, oder extern, d.h. außerhalb des Unternehmens, zu unterscheiden; (2) Wie werden die Daten genutzt? Auch in diesem Kontext lässt sich eine interne Datennutzung, d.h. Nutzung der Daten innerhalb des Unternehmens, von einer externen Datennutzung, d.h. Nutzung der Daten außerhalb des Unternehmens, unterscheiden. Je nach Einordnung des Anwendungsfalls lassen die beiden Einordnungskriterien Datenherkunft und Datennutzung ein Einordnungsschema mit vier zu unterscheidenden Arten der Datenbewirtschaftung zu. Abbildung 1 gibt einen Überblick zur Einordnung der vier verschiedenen Arten der Datenbewirtschaftung und ihrer Anwendungen.

Abbildung 1: Einordnungsschema für die Arten der Datenbewirtschaftung

Datenherkunft / Datennutzung	Intern	Extern
Intern	Product Maintenance (A)	Produktentwickler (D) Anlagendienstleister (E)
Extern	Datenverkäufer (B) Datenpool (C)	Plattformbetreiber (F)

Datenherkunft / Datennutzung	Intern	Extern
Intern	Product Maintenance (A)	Produktentwickler (D) Anlagendienstleister (E)
Extern	Datenverkäufer (B) Datenpool (C)	Plattformbetreiber (F)

Zur Argumentation der unterschiedlichen Rechtsfragen soll eine Orientierung an der Art der Datenherkunft erfolgen, die intern oder extern sein kann. Bei der internen Datenherkunft werden eigene Daten genutzt, bei denen sich unmittelbar aus der faktischen Herrschaft über die Daten die Verwendungsmöglichkeiten für den Dateninhaber ergibt. Die externe Datenherkunft geht hingegen mit einer Übertragung der Daten einher, an die sich weitere rechtliche Fragen der Datennutzung anschließen.

1. Interne Datennutzung

Unternehmen A – Product Maintenance. Unternehmen C nutzt eigene (Fertigungs-) Daten, um die betriebsinternen Fertigungsabläufe zu optimieren (sog. Product Maintenance). So lassen sich über Sensoren Daten erheben und auswerten, die Produktionsausfälle verhindern, mehrstufige Fertigungsprozesse durch eine effiziente Verzahnung der unterschiedlichen Produktionsschritte schneller und effizienter gestalten sowie anstehende Wartungsarbeiten oder der Austausch von Verschleißteilen vorhersagen. Die Daten stammen dabei aus internen Datenquellen, weil über Sensoren in den eigenen Fertigungsanlagen Daten gesammelt und ausgewertet werden. Gerade kleinere Unternehmen könnten die Datenanalyse auch an externe Dritte auslagern, wenn beispielsweise die unternehmensinternen Kapazitäten oder Mitarbeiterkompetenzen nicht ausreichen, um die Auswertung eigenständig zu übernehmen. In einem solchen Fall würden die Daten extern genutzt, auch wenn die Auswertungsergebnisse intern z.B. zur Optimierung der betriebsinternen Produktionsabläufe und -prozesse genutzt werden.

Unternehmen B – Datenverkäufer. Unternehmen E sammelt Daten (z.B. Mobilfunkdaten, Verkehrsdaten, Klimadaten usw.), um diese auf einem Datenmarktplatz zum Kauf anzubieten. Hier stammen die Daten aus internen Datenquellen, weil die Daten mithilfe von Sensoren eigenständig generiert, gesammelt und gespeichert werden. Diese Daten nutzt das Unternehmen E ausschließlich zum Verkauf an externe Dritte (z.B. als Trainingsdaten für KI-Systeme), sodass die Datennutzung ausschließlich extern erfolgt.

Unternehmen C – Datenpool(-betreiber). Unternehmen F benötigt unterschiedliche Datenquellen, um ein KI-System zu trainieren und teilt vor diesem Hintergrund mit anderen Anbietern in der Domäne einen Datenpool. Für die benötigte Infrastruktur

greift das Unternehmen F dabei auf GAIA-X zurück. Um die Datenvielfalt möglichst breit zu gestalten, ist der Datenpool als offener Pool ausgestaltet, d.h. andere Anbieter können ohne Eintrittsbarriere am Datenpool teilhaben, sofern diese ein Mindestmaß an eigenen nützlichen Daten ebenfalls im Datenpool teilen.

2. Externe Datennutzung

Unternehmen D – Produktentwickler. Unternehmen A nutzt Daten (externe Datenherkunft) für die Produktentwicklung im Rahmen eines datengetriebenen Geschäftsmodells. Ein typisches Beispiel für ein solches datengetriebenes Produkt ist das autonome Fahrzeug. Die für das Training des zugrundeliegenden Systems Künstlicher Intelligenz (KI) verwendeten Daten stammen in der Regel aus externen Quellen und enthalten beispielsweise Bilder von möglichen Gefahrenquellen im Straßenverkehr (Großvieh, Bäume usw.). Daneben kann das Unternehmen A die beim Fahren gesammelten Daten zum „Weiterlernen" nutzen (Connected Cars).

Unternehmen E – Anlagendienstleister. Unternehmen B ist Anlagenhersteller und produziert Fertigungsmaschinen für die verarbeitende Industrie. Neben der Herstellung der Fertigungsanlagen bietet das Unternehmen B additive Anlagendienstleistungen an. Über verbaute Sensoren in den Anlagen können Datenanalysen Aussagen und Beratungen hinsichtlich der Optimierung, der kostenreduzierenden Wartung der Maschinen usw. getroffen werden. Die Daten stammen dabei aus externen Quellen, weil die Anlagenmaschinen bei den Kunden in Betrieb sind und im laufenden Fertigungsprozess Daten gesammelt werden. Das Unternehmen nutzt diese Daten zu internen Zwecken, um weitere Dienstleistungen gegen ein Entgelt anzubieten. Zu berücksichtigen ist dabei, dass z.B. über Aufzeichnungen des Namens oder der Personalnummer des Fahrzeugführers die Daten einen Personenbezug bekommen können. In besonders spezialisierten Bereichen muss hierzu nicht einmal der konkrete Name des Fahrzeugführers erfasst werden, weil durch eine besondere Ausbildung eines einzelnen Mitarbeiters oder den Urlaubs- und/oder Schichtplan auf den Fahrzeugführer geschlossen werden kann.

Unternehmen F – Plattformbetreiber. Unternehmen D ist Betreiber einer (Internet-) Plattform für den Datenkauf und -verkauf. Hier stammen die Daten typischerweise aus externen Datenquellen und werden wiederum von anderen externen Dritten genutzt. Unternehmen D ist also lediglich ein Intermediär, der Käufer- und Verkäuferseite zusammenbringt. Die Plattform erlaubt neben Verknüpfungen zu externen Cloud-Diensten auch das (temporäre) Speichern von Daten in der Cloudlösung der Plattform.

III. Rechtliche Analyse

1. Drei-Ebenen-Modell

In der juristischen Diskussion werden die Bezugspunkte einer Regulierung von Daten zumeist nach einem Drei-Ebenen-Modell unterschieden.[5] Auf der physischen/strukturellen Ebene befinden sich Regelungen, die an die Verkörperung von Daten

---

[5] Grundlegend *Zech,* Information als Schutzgegenstand, 2012, S. 37 ff. Auf die syntaktische Ebene beschränkt die zivilrechtliche Definition hingegen *Denga*, NJW 2018, 1371.

anknüpfen, also an den Datenträger.[6] Die semantische Ebene wird von Regelungen betroffen, die sich auf den Inhalt der digital lesbaren Information beziehen. Gleichsam dazwischen liegt die syntaktische Ebene, die die maschinenlesbare Codierung der (semantischen) Information bezeichnet.

In den bekannten digitalen Geschäftsmodellen stehen diese Ebenen freilich nicht unverbunden nebeneinander. Eine Datenökonomie baut zumeist auf den semantischen Informationen auf, benötigt diese aber gerade in digitaler Syntax, die wiederum ohne eine Speichermöglichkeit nur flüchtig wäre. Zudem bilden die gesetzlichen Vorgaben im Hinblick auf alle drei Ebenen den Hintergrund des Datenvertragsrechts, ebenso wie das Sachenrecht des BGB den Hintergrund des Schuldrechts bildet. Ein Datenlizenzvertrag (gleich welcher Natur) muss daher typischerweise alle drei Ebenen beachten und darf den Blick nicht zu sehr auf eine der Ebenen verengen. Der Vertrag muss folglich Regelungen für alle Ebenen enthalten oder jedenfalls bedenken.

Und schließlich bestimmen die gesetzlichen Vorgaben damit auch, welche Parteien an einer vertraglichen Vereinbarung zu beteiligen sind. Bestehen Verbots- oder Ausschließlichkeitsrechte zugunsten eines Dritten, können ggf. keine durchsetzbaren Rechte ohne dessen Zustimmung übertragen, eingeräumt oder erworben werden. Solche Verbotsrechte können sich wiederum vor allem aus der Inhalts- oder Strukturebene der Daten ergeben. Besonders problematisch wird es dabei, wenn Ausschließlichkeitsrechte auf mehreren Ebenen bestehen und die Rechtspositionen unterschiedlichen Rechtsinhabern zufallen. Dann bedarf es eines Ausgleichs der Rechte untereinander und sind ggf. mehrere Dritte zu berücksichtigen.

2. Personenbezogene vs. nicht-personenbezogene Daten

Das Ausmaß und die Dichte der Regelung spezifisch von Daten unterscheidet sich deutlich für personenbezogene und nicht-personenbezogene Daten. Während erstere detaillierten, spezifischen Regeln unterworfen sind, fehlen solche für letztere weitgehend.

a) Personenbezogene Daten

Personenbezogene Daten werden auf mehreren Ebenen von geschriebenen Normen erfasst. Zuerst bestimmen Art. 8 GRCh und Art. 16 AEUV, dass jede Person ein Recht auf Schutz ihrer personenbezogenen Daten hat und legen einige weitere Regeln hierfür fest. Ergänzt wird dies von Art. 7 GRCh und Art. 8 EMRK um den Schutz des Privatlebens und der persönlichen Kommunikation. In Art. 16 Abs. 2 und 39 AEUV finden sich zudem Ermächtigungsgrundlagen für den Erlass von konkretisierenden Rechtsakten. Davon hat die Union durch Erlass der DSGVO[7], der Datenschutz-Richtlinie für

---

[6] Als einen Nebenaspekt der physischen Ebene kann man die informationstechnische „logische“ Ebene ansehen. Damit ist gemeint, dass in manchen Speichersystemen Daten mehrfach abgelegt werden, ohne dass der Benutzer auf diese Kopien gezielt und separat zugreifen könnte, weil sie vom IT-System (technisch) als Einheit angesehen werden, vgl. *Riehm,* VersR 2019, 714, 715

[7] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. 2016 Nr. L 119/1.

Elektronische Kommunikation[8] sowie der JI-RL[9] Gebrauch gemacht. Daneben gewährleisten im nationalen Recht das Grundrecht auf informationelle Selbstbestimmung und das allgemeine Persönlichkeitsrecht, dass der Einzelne grundsätzlich selbst über die Verwendung seiner personenbezogenen Daten entscheiden kann.[10]

Gemäß Art. 4 Nr. 1 DSGVO sind personenbezogene Daten „alle 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." Wegen dieser weiten Definition ist auch bei industriell oder maschinell erhobenen Daten stets zu prüfen, ob nicht doch ein Personenbezug besteht. Dafür genügt – wie oben schon gezeigt – auch der Bezug zu Mitarbeitern des datenerhebenden Unternehmens, die Maschinen oder Fahrzeuge bedienen. Häufig werden daher doch die Voraussetzungen von Art. 4 Nr. 1 DSGVO erfüllt sein.[11] Auch eine spätere Anonymisierung hilft hier nicht immer, denn es bedarf jedenfalls bereits einer Ermächtigungsgrundlage zur Erhebung der später anonymisierten Daten.

b) Nicht-personenbezogene Daten

Die hier im Fokus stehenden nicht-personenbezogenen Daten sind solche, bei denen ein Personenbezug nach Art. 4 Nr. 1 DSGVO gerade nicht vorliegt. Hierunter können z.B. fallen 3D-Druck-Daten, Mess- und Produktionsdaten in der vernetzten Produktion12, Verschleiß- und Wartungsinformationen zu Produktionsmitteln oder hinreichend aggregierte und anonymisierte Datensätze[13]. Häufig wird in diesem Zusammenhang auch die Präzisionslandwirtschaft genannt.[14] Die Regeln des Umgangs mit diesen Daten sind nicht ebenso eingehend gesetzlich spezifiziert wie die hinsichtlich personenbezogener Daten.

Gleichwohl lassen sich gerade in jüngerer Zeit zunehmend Normierungsbestrebungen ausmachen, die sich einer „Daten-Governance" zuordnen lassen. Neben der

---

8 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste erzeugt oder verarbeitet werden, ABl. 2006 Nr. L 105/54.

9 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung, ABl. 2016 Nr. L 119/89.

10 Zur Abgrenzung der Schutzbereiche der beiden Grundrechte s. *Brink,* in BeckOK Datenschutzrecht, 30. Ed. 1.11.2017, Syst. C Rn. 59.

11 *Steinrötter,* FS Taeger, 2020, 491, 498; *Specht,* ZGE/IPJ 9 (2017), 411.

12 KOM, „Aufbau einer Europäischen Datenwirtschaft", COM(2017) 9 final, S. 10.

13 *Behling,* ZGE 2021, 3, 7; *Hacker,* ZGE 2020, 239, 246 ff.

14 BE 9 VO (EU) 2018/1807.

Datenverkehrsverordnung[15] sind das vor allem die PSI-Richtlinie[16] und Art. 6 VO (EU) 2018/1807. Der Schwerpunkt dieser Vorschriften liegt jedoch auf der Schaffung spezifischer Zugangsrechte Einzelner zu spezifischen Daten und nicht einer kohärenten Regelung eines Datenwirtschaftsrechts[17]. Dieser Befund dürfte sich auch angesichts des Vorschlags einer Verordnung über europäische Daten-Governance[18] nicht grundlegend ändern, weil es diesem an zwingend harmonisierenden Vorgaben mangelt.[19]

Darüber hinaus unterliegt die Bewirtschaftung von nicht-personenbezogenen Daten den allgemeinen Regeln des Wirtschaftsrechts. Aus ihnen sind daher die Regeln eines B2B-Datenvertragsrechts zu entwickeln. Die Vorgaben für Verträge über digitale Produkte nach der Digitale-Inhalte-Richtlinie[20] und deren Umsetzung in §§ 327 ff. BGB können hierfür nur begrenzt Pate stehen, weil sie spezifisch verbraucherschützend konzipiert und im Wesentlichen auf vertragsrechtliche Gewährleistungsrechte beschränkt sind.

3. Daten als Objekt faktischer Herrschaft

Im Zentrum der hiesigen Erörterungen soll das Datenvertragsrecht stehen. Gleichwohl darf nicht übersehen werden, dass jenes auf bestehenden ausschließlichen Nutzungsrechten aufbauen würde.[21] Existierende dingliche Zuordnungsregeln würden sich auf der vertraglichen Ebene zumindest als *default rules* darstellen und deshalb Aktivitäts- und Verhandlungslasten verteilen.[22] Das Vertragsrecht mag daher zwar die praktischen Probleme einer „Datenlizenz" adressieren können,[23] es folgt jedoch anderen Logiken als es dingliche Zuordnungsrechte tun.

---

15 Verordnung (EU) 2018/1807 des Europäischen Parlaments und des Rates vom 14. November 2018 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union, ABl. 2018 Nr. L 303/59.

16 Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors, ABl. 2019 Nr. L 172/56.

17 Zur Emergenz dieses Rechtsgebiets *Steinrötter,* FS Taeger, 2020, S. 491 ff.; *ders.,* RDi 2021, 480 ff.

18 COM(2020) 767 final.

19 Ebenso *Spindler,* CR 2021, 98, 102.

20 Richtlinie (EU) 2019/770 des europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, ABl. 2019 Nr. L 136/1.

21 Zutreffend *Behling,* ZGE 2021, 3, 21.

22 Grundlegend aus rechtsökonomischer Sicht zu den Default Rules sind die Arbeiten von *Ronald Coase* zur Transaktionskostenökonomik sowie den handelbaren Nutzungsrechten im Rahmen des sog. Coase-Theorems, siehe *Coase,* The Problem of Social Cost, Journal of Law and Economics 1960, 1-44. Vor diesem Hintergrund sind es die Transaktionskosten, die einer marktlichen Lösung entgegenstehen, und die durch einfache dispositive Normen (default rules) so gesenkt werden könnten, dass kein weiterer staatlicher Eingriff notwendig wird (*Scheufen,* Angewandte Mikroökonomie und Wirtschaftspolitik - Mit einer Einführung in die ökonomische Analyse des Rechts, 2020). Zum Verhältnis von Markt versus Staat prägen *Cooter/Ulen* in diesem Zusammenhang die Unterscheidung zwischen dem normativen Coase-Theorem und dem normativen Hobbes-Theorem, vgl. *Cooter/Ulen,* Introduction to Law and Economics, 5. Auflage 2007 (1. Auflage 1996), S. 96 ff.

23 Vgl. COM(2018) 232 final, S. 11; ebenso *Steinrötter,* FS Taeger, 20202, S. 491, 507 f.; *Berger,* ZGE/IPJ 9 (2017), 340, 350 f. *Faust,* Digitale Wirtschaft – Analoges Recht, Gutachten für den 71. DJT, 2016, A 10; in diesem Sinne auch *Kraul,* GRUR-Prax 2019, 478, 479.

a) Eigentumsrechtliche Schutzdimensionen

Die strukturelle Ebene von Daten, der Datenträger, ist Sache iSv § 90 BGB.[24] Demgegenüber sind Daten „an sich", also im Hinblick auf ihre syntaktische und semantische Ebene keine körperlichen Gegenstände und damit keine Sachen iSv § 90 BGB. Anders als an ihnen kann am Datenträger unproblematisch Eigentum iSv § 903 BGB[25], Besitz iSv § 854 BGB[26] oder ein Pfandrecht iSv § 1204 BGB begründet werden. Zudem ergeben sich keine Besonderheiten daraus, ob der Datenträger mit Daten „beschrieben" ist oder nicht.[27] Der sachenrechtliche Schutz von Daten beschränkt sich auf deren strukturelle Ebene, aus dem Eigentum am Datenträger folgt nicht automatisch ein Recht an dessen Inhalten.[28] Aus der Eigentumsebene ergeben sich aber reflexartig auch Beschränkungen für die Nutzung der syntaktischen und semantischen Ebene von Daten.

So kann der Eigentümer nach § 1004 BGB jede Veränderung des Datenträgers abwehren. Ein datenverändernder Zugriff kann daher vom Eigentümer untersagt werden. Fraglich ist zudem, ob der Eigentümer des körperlichen Datenträgers schon aufgrund von § 903 S. 1 BGB andere von dem bloßen Zugang zum Datenträger und seiner Nutzung – auch aufgrund eines informationstechnischen Fernzugriffs – ausschließen kann. Die Frage ist hier nicht, ob der Eigentümer eines Datenträgers ein „Recht an den darauf verkörperten Daten" hat,[29] sondern ob er aus der Eigentümerstellung heraus den Zugriff auf sein informationstechnisches System dulden muss. Mit Blick auf die Funktionsweise eines Fern-/Datenabrufs muss das verneint werden.[30] Sieht man jegliche Einwirkung auf eine Sache als Beeinträchtigung des Eigentums nach § 1004 S. 1 BGB an,[31] ergäbe es sich schon hieraus.[32] Dem wird entgegengehalten, dass nur nicht-rivale Nutzungen dem Eigentümer nach § 903 S. 1 BGB exklusiv zugewiesen seien.[33] Deshalb soll zwar das Löschen oder Verändern der Daten vom Schutz des Eigentumsrecht umfasst sein, nicht aber das bloße Auslesen derselben (insb. mit dem Ziel der Erstellung einer Kopie).[34] Für dieses Verständnis spricht hingegen jedenfalls keine Parallele zum Fotografieren von Gebäuden,[35] denn dort werden lediglich Lichtwellen aufgefangen, die – ohne Zutun eines der Beteiligten – auf das Aufnahmegerät des Fotografierenden treffen. Demgegenüber setzt der Fernzugriff auf einen Datenträger stets eine

---

24 BeckOK BGB/*Fritzsche,* 59. Ed. 1.8.2021, BGB § 90 Rn. 27.

25 MüKoBGB/*Wagner*, 8. Aufl. 2020, BGB § 823 Rn. 246;

26 BGH NJW 2016, 1094 Rn. 20; BeckOGK/*Götz*, 1.1.2022, BGB § 854 Rn. 31.

27 Zur Frage, ob das Beschreiben des Datenträgers die Eigentumszuordnung ändern kann BGH NJW 2016, 317 Rn. 11 mwN.

28 BGH NJW 2016, 317 Rn. 20.

29 Missverständlich insofern z.B. *Zech,* AcP 219 (2019), 488, 586.

30 Ebenso *Raue,* NJW 2019, 2425, 2426 und 2427 f. (gerade unter Berufung auf die Preußische-Schlösser-und-Gärten-Rechtsprechung des BGH); *Behling,* ZGE 2021, 3, 23; in der Sache auch *Riehm,* VersR 2019, 714, 721; das Abstellen auf eine „Fühlungnahme" lehnt *Zech,* AcP 219 (2019), 488, 559 ff. ausdrücklich ab.

31 Vgl. BeckOK BGB/*Fritzsche,* 59. Ed. 1.8.2021, BGB § 1004 Rn. 32, 34.

32 Arbeitsgruppe „Digitaler Neustart", Bericht vom 15. Mai 2017, S. 38 Rn. 55; *Heun/Assion,* CR 2015, 812, 817; *Assion* CR 2016, 83, 84.

33 *Zech,* AcP 219 (2019), 488, 577 ff.; *Zech*, Information als Schutzgegenstand, 2012, S. 274 ff.; zust. MüKoBGB/*Wagner,* 8. Aufl. 2020, § 823 Rn. 246, 254.

34 *Specht,* CR 2016, 288, 292; *Zech,* CR 2015, 137, 141 f.; *Zech,* AcP 219 (2019), 488, 585; *Härting,* CR 2016, 646, 647. Nicht jeder Nur-Lesezugriff auf eine digitale Datei erfolgt technisch nicht-rival, so dass sogar ein vorübergehender Ausschluss der Nutzung des Eigentümers möglich ist; darauf stellt entscheidend ab *Riehm,* VersR 2019, 714, 721.

35 So aber *Zech,* Information als Schutzgegenstand, 2012, S. 118.

physische Verbindung mit diesem oder anderer, vermittelnder Hardware des Eigentümers voraus. Außerdem müssen bei einem Fernzugriff die zu lesenden oder zu kopierenden Daten auf Anfrage erst vom System des Eigentümers gesendet werden.

b) Vielfältiger Schutz der Semantik

Auch die inhaltliche Ebene kann Bezugspunkt zahlreicher rechtlicher Regelungen sein. Die rechtlichen Regelungen knüpfen hierbei nicht an die digitale Syntax der Daten, sondern an deren semantische Bedeutung an.

Hierbei ist zu beachten, dass die Zahl der anwendbaren Regelungsregime potentiell unbegrenzt ist. Der Datenbegriff beschränkt gerade die erfassten Inhalte nicht. Er schließt damit jeglichen Austausch digitaler Inhalte, Produkte und Dienstleistungen ein, aber eben auch schlichte tagesaktuelle politische oder rein technische Information (z.B. Wetterdaten). Erfasst werden deshalb beispielsweise nicht nur die Nutzung eines sozialen Netzwerks oder der Zugriff auf eine Onlinezeitung, sondern auch das Streaming von Filmen oder Musik, digitales Fernsehen oder Rundfunk, der Verkauf von Computerspielen oder E-Books, die digitale Übermittlung eines anwaltlichen Gutachtens oder medizinischer Testergebnisse sowie der Verkauf von Adress- oder Bonitätsinformationen. Sogar analoge Sachverhalte werden vom Datenbegriff nicht ausgeschlossen,[36] wenngleich dort in der Datenwirtschaft faktisch kein Schwerpunkt liegen mag. Es gilt aber darüber hinaus, dass eine digitalisierte und internetbasierte Wirtschaft technisch immer auch eine datenbasierte Wirtschaft ist. So vielfältig wie die digitalisierten Informationen sind auch die potentiell auf diese Informationen anwendbaren Rechtsregime. Bei den hier interessierenden Maschinendaten kommt vor allem ein Schutz als Datenbank oder Geschäftsgeheimnis in Betracht.

c) Schutz der Syntax: Kein originäres Datenausschließlichkeitsrecht

An der Syntax von Daten bestehen regelmäßig keine urheberrechtlichen Rechte. Dateiformate selbst sind regelmäßig nicht als Computerprogramme geschützt.[37] Werkschutz nach § 2 Abs. 2 UrhG ist nicht per se ausgeschlossen,[38] dessen Voraussetzungen sind jedoch regelmäßig nicht erfüllt.[39] Der innere Aufbau eines Dateiformats kann ein Geschäftsgeheimnis iSd GeschGehG sein, wenn dieser von entsprechenden Geheimhaltungsmaßnahmen betroffen ist.

Zudem ist es die syntaktische Ebene, die im Zentrum der Diskussion um ein „Dateneigentum“, ein „Datenausschließlichkeitsrecht“[40] steht. Hierbei geht es um die Frage, ob es einer originären ausschließlichen Zuordnung der Nutzungsbefugnis an Daten zu einer oder mehreren Personen bedarf und nach welchen Grundsätzen diese Zuordnung ggf. vorzunehmen ist. Mit der Maschinenlesbarkeit wird an den Umstand angeknüpft, dass die Daten in der digitalen Wirtschaft wertschöpfend verwendet

---

36 Anders z.B. *Markendorf,* ZD 2018, 409, 410, der an den Datenbegriff von § 202a Abs. 2 StGB anknüpft.

37 Spindler/Schuster/*Wiebe,* 4. Aufl. 2019, UrhG § 69a Rn. 19.

38 Vgl. EuGH v. 2.5.2012 – C-406/10, *ECLI:EU:C:2012:259 – SAS Institute,* Rn. 45.

39 *Marly,* GRUR 2012, 773, 779; Spindler/Schuster/*Wiebe,* 4. Aufl. 2019, UrhG § 69a Rn. 19.

40 Für den Begriff des „Eigenrechts“ *Berger,* ZGE/IPJ 9 (2017), 340, 348.

werden können.[41] So würde auch sichergestellt, dass die Daten unabhängig von ihrem konkreten Inhalt schutzfähig sind.

Soweit die Literatur einem solchen Ausschließlichkeitsrecht nicht generell ablehnend gegenübersteht,[42] kommen unterschiedliche normative Anknüpfungspunkte und Vorgehensweisen in Betracht. Gegen eine Analogie zum Besitzrecht[43] wird zu Recht eingewendet, dass aus dem possessorischen Besitzschutz des BGB gerade keine endgültige Zuordnung von Nutzungsrechten folgen soll.[44] Der Datenintegritätsschutz des § 823 Abs. 1 BGB knüpft an das Eigentum am Träger an und lässt sich allenfalls auf den Transport von Daten auch auf fremden Datenleitungen erweitern.[45] Zudem zeigt sich, dass die Person des originären Rechtsinhabers letztlich doch stets nach unabhängigen Wertungsgesichtspunkten bestimmt wird.[46]

Mangels passender Analogiegrundlagen kann ein solches Recht daher nur durch den Gesetzgeber geschaffen werden.[47] Hier ist jedoch nicht der Ort, um die Sinnhaftigkeit und Ausgestaltung eines solchen, zu schaffenden Ausschließlichkeitsrechts an Daten zu diskutieren.[48]

d) Faktische Herrschaft und Zugangskontrolle maßgeblich

Als Zwischenergebnis ist daher festzuhalten: Abgesehen von besonderen Konstellationen besteht derzeit an nicht-personenbezogenen Daten kein ausschließliches Herrschafts- oder Nutzungsrecht. Die Nutzung solcher Daten ist also grundsätzlich frei und ohne Erlaubnis einer anderen Person möglich. Es existieren keine spezifischen zivilrechtlichen Schranken dafür, einmal erlangte Rohdaten zu verwenden. Zu beachten bleibt aber, dass potentiell jedes subjektive Recht an der Struktur, Syntax oder Semantik der Daten den Inhaber dieses Rechts berechtigen kann, andere von der Einwirkung auf oder der Nutzung von diesen Daten auszuschließen.

Spiegelbildlich ist es damit auch die faktische Herrschaft über den Datenträger und den technisch-physischen Zugang zu ihm, die die Möglichkeit zur Datennutzung steuert und eine wirtschaftliche Vorzugsstellung begründet.[49] Wer einen Datenträger an einen anderen Ort bringen kann oder den physischen Zugang verhindern kann, oder wer

---

41 *Zech*, Information als Schutzgegenstand, 2012, S. 422 ff.; *KOM,* Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, SWD(2017) 2 final, S. 34.

42 So z.B. *Steinrötter,* FS Taeger, 2020, S. 491, 507 f.; *Zech,* Besitz an Daten?, in Pertot (Hrsg.), Rechte an Daten, 2020, S. 91 ff.; *Determann,* ZD 2018, 503 ff.; *Heymann,* CR 2016, 650 ff.; *Dorner,* CR 2014, 617, 626 f.; *Kühling/Sackmann,* ZD 2020, 24, 26; wohl auch *Schweitzer,* GRUR 2019, 569, 570 (keine Reduzierung der Komplexität zu erwarten).

43 Insb. *Hoeren,* MMR 2019, 5 ff.; an die faktisch-technische Zugriffsberechtigung knüpft auch *Adam,* NJW 2020, 2063 Rn. 12 ff., 28 ff. an.

44 *Weiß,* ZD 2020, 161; OLG Brandenburg, NJW-RR 2020, 54 Rn. 42.

45 In diesem Sinne *Riehm,* VersR 2019, 714, 720 ff.

46 Vgl. *Fezer,* MMR 2019, 3, 4 f.; *Hoeren,* MMR 2019, 5, 7; *Riehm,* VersR 2019, 714, 722; *Markendorf,* ZD 2018, 409, 410 f.; *Specht*, CR 2016, 288, 291; *Kornmeier/Baranowski,* BB 2019, 1219, 1223. S. a. *Steinrötter,* FS Taeger, 2020, S. 491, 508; deswegen auch krit. *Heymann,* CR 2016, 650, 654; *Adam,* NJW 2020, 2063, 2064.

47 *Fritzsche,* FS Harte-Bavendamm, 2020, S. 33, 38; *Zech,* CR 2015, 137, 145 f.

48 Dazu z.B. *Behling,* ZGE 2021, 3 ff.

49 In diesem Sinne auch *Hacker,* GRUR 2020, 1025, 1032; *Fritzsche,* FS Harte-Bavendamm, 2020, S. 33, 39; *Riehm,* VersR 2019, 714, 720; *Kühling/Sackmann,* ZD 2020, 24, 26 f.; *Schweitzer,* GRUR 2019, 569, 575; *Zech,* CR 2015, 137, 140; *Schur,* Die Lizenzierung von Daten, 2020, S. 157; *Kristl,* MMR 2021, 386, 388.

dessen Adresszuordnungen im world wide web verändern oder den Fernzugriff blockieren kann, der kontrolliert auch den Zugang zu den auf dem Träger enthaltenen Daten und damit mittelbar auch deren Verwendungsmöglichkeiten. Ist aber die physische Kontrolle des Datenträgers maßgeblich, gewinnen die dinglichen und obligatorischen Rechten am selben an Bedeutung. Dann kommt es möglicherweise allein darauf an, sich möglichst früh einen (informations)technisch-physischen Zugang zu dem Punkt zu sichern, an dem die Daten entstehen. Technische Schutzmaßnahmen können diese faktische Ausschlussposition noch verstärken.[50] So kann der Einsatz von Verschlüsselungstechniken oder proprietären Dateiformaten den Zugriff anderer Personen auf die Daten und deren semantischen Gehalt verhindern.

Diese Datenherrschaft genügt zudem für eine rechtmäßige, also nicht-rechtswidrige Datenverarbeitung. Daraus folgt zwar immer noch keine positive (exklusive) Zuweisung der Nutzungsmöglichkeit,[51] aber sie ist eben auch nicht Dritten positiv zugewiesen.[52] Aus der faktischen Ausschließbarkeit folgt nämlich keine rechtliche Ausschließlichkeit.[53] Die Datennutzung ist dem Herrschaftsinhaber gleichsam freigestellt. Dementsprechend hat der BGH in früheren Entscheidungen ausgeführt, dass die Innehabung von Daten und das Recht, diese zu nutzen, mit der tatsächlichen Herrschaft über den Datenträger herausgegeben werden kann.[54]

Im Einklang mit diesen Grundsätzen darf der Datenverwender auch sämtliche Erträge und Gewinne aus der Datenverarbeitung behalten. An aus den Daten erzeugten weiteren Daten steht ihm gleichwohl ebenso keine ausschließliche Rechtsposition zu.

4. Datennutzungsverträge

In einer freien Marktwirtschaft sollten privatautonome Regelungen im Vordergrund stehen. Vorrangiges Mittel der privatautonomen Gestaltung der eigenen Rechtsverhältnisse ist der Vertrag. Es ist allgemein anerkannt, dass die Inhaberschaft und Nutzungsberechtigung von Daten Gegenstand von Verträgen sein kann.[55] Im Folgenden sollen daher die für solche Verträge besonders relevanten Gesichtspunkte dargestellt und auf die eingangs aufgegriffenen Beispiele angewendet werden.

a) Vorüberlegungen und Vertragstypologie

Ein Vorteil vertraglicher Vereinbarungen liegt darin, dass diese die konkreten Bedürfnisse der beteiligten Parteien oftmals besser und passgenauer abbilden können als pauschale gesetzliche Vorgaben.[56] Gleichzeitig binden Schuldverträge aber nur

---

50 *Heymann,* CR 2016, 650, 652.

51 A.A. *Riehm,* VersR 2019, 714, 720: „aus der initialen faktischen Zugriffsmöglichkeit auf gespeicherte Daten durch denjenigen, der sie als erstes gespeichert hat," folgt auch eine Zuweisung an ihn.

52 *Schefzig,* Die Datenlizenz, in: Taeger (Hrsg.), Internet der Dinge, 2015, S. 551, 556 f.

53 Missverständlich daher *Kornmeier/Baranowski,* BB 2019, 1219, 1223 oder *Kühling/Sackmann,* ZD 2020, 24, 27; wie hier *Kraus,* Datenlizenzverträge, in: Taeger (Hrsg.), Internet der Dinge, 2015, S. 537, 539; *Schur,* Die Lizenzierung von Daten, 2020, S. 157; zur Domain ebenso BGH GRUR 2005, 969, 970.

54 BGH NJW 1996, 2159, 2161; ähnlich auch BGH NJW 2016, 1094 Rn. 20.

55 Ausdrücklich statt aller z.B. BeckOK BGB/*Fritzsche,* 59. Ed. 1.8.2021, BGB § 90 Rn. 30.

56 *Steinrötter,* FS Taeger, 2020, S. 491, 499; *Kornmeier/Baranowski,* BB 2019, 1219, 1221.

diejenigen Personen, die sie abgeschlossen haben. Fehlt es – wie im Bereich der Datenwirtschaft – an einer allgemeinen dinglichen Rechtsposition, die auf Basis von Verträgen übertragen oder eingeräumt werden kann, so verschafft ein Vertrag keine gegenüber Dritten gesicherten Rechtspositionen.[57] Zwar können zugunsten Dritter auch Rechte gegen die Vertragsparteien eingeräumt werden, eine Handhabe gegen ungewollten Zugang zu oder ungewollte Nutzung von Daten durch Dritte bietet ein Vertrag dann jedoch nicht.[58]

(Datenlizenz-)Verträge können freilich auch vor dem Hintergrund der oben skizzierten rechtlichen Unsicherheit im Hinblick auf die dingliche Rechtslage geschlossen werden. Dann muss der Fokus auf einer offenen Formulierung der Vertragsklauseln liegen, die auf alle potentiellen Ausgangsrechtslagen Rücksicht nimmt. Hierbei ist naturgemäß das Risiko einer ungewollten ex-post-Auslegung größer, als wenn die Rechtspositionen, die den Beteiligten eingeräumt werden sollen, bestimmt und konkret bezeichnet werden (können). Angesichts der funktionsorientierten Auslegung von Verträgen und den größeren Spielräumen im Unternehmerverkehr können hierbei aber ausführliche Präambeln und eingehende Zweckbestimmungen hilfreich sein.[59] Aber auch unabhängig davon stellt sich – wie stets – für die Kautelarpraxis die Herausforderung, im Vertrag alle wesentlichen Konstellationen und Probleme zu adressieren.[60]

Schließlich liegt eine Grenze der vertraglichen Gestaltungsoptionen in der negativen Vertragsfreiheit. Danach kann ein Rechtssubjekt regelmäßig nicht gezwungen werden, einen (bestimmten) Vertrag abzuschließen. Der Wille zum Teilen der Daten muss also beim Dateninhaber bereits vorhanden sein (oder sich durch ökonomische Anreize wecken lassen können).[61]

Eine abschließende Aufzählung aller für die Datenwirtschaft in Betracht kommenden Verträge ist nicht zu leisten, denn schon die eingangs skizzierten Beispiele zeigen eine große Vielfalt an möglichen Interessenkonstellationen. Ausgehend von diesen lassen sich aber Grundtypen von Datenverträgen ausmachen. An diesen Grundtypen können dann nicht nur die wesentlichen Strukturmerkmale des jeweiligen Vertrags ausgerichtet werden, sondern sie dürften auch Grundlage für die Maßstabsbildung des zwingenden Rechts und der Inhaltskontrolle sein, insbesondere für die §§ 305 ff. BGB.

Maßgeblich für die Typisierung eines Vertrages sind die von den Parteien vereinbarten Hauptleistungspflichten. Decken sich diese im Wesentlichen mit gesetzlich normierten oder in der Praxis ausgeformten Vertragstypen, so ist die Vereinbarung entsprechend zuzuordnen. Was vereinbart ist, bestimmt sich gemäß §§ 133, 157 BGB zuerst nach dem übereinstimmenden Willen der Parteien und nicht nach der gewählten Bezeichnung des Vertrages.[62] Der Wortlaut der Vereinbarung ist freilich wesentlicher Anhaltspunkt für die subsidiäre Auslegung nach dem objektiven Empfängerhorizont.[63]

---

57 *Hessel/Leffer,* MMR 2020, 647, 648.

58 *Berger,* ZGE/IPJ 9 (2017), 340, 351.

59 Allgemein dazu *Döser,* JuS 2000, 456 f.; *Schneider* in: Schneider (Hrsg.), Handbuch EDV-Recht, 5. Aufl. 2017, M. Rn. 653 ff.; BeckOGK/*Möslein*, 1.10.2020, BGB § 133 Rn. 56.

60 *Hessel/Leffer,* MMR 2020, 647, 648.

61 *Fritzsche,* FS Harte-Bavendamm, 2020, S. 33, 44.

62 BGH NJW 2002, 3317, 3318.

63 MüKoBGB/*Busche,* 9. Aufl. 2021, § 133 Rn. 68; ähnlich BeckOGK/*Möslein,* 1.10.2020, BGB § 133 Rn. 50.

aa) Vereinbarungen über die Dateninhaberschaft

Mangels einer allgemeinen, verbindlichen Zuweisung von Daten an ein bestimmtes Rechtssubjekt lassen sich zuerst Vereinbarungen über die Dateninhaberschaft finden.[64] Treffend wurden solche Abreden als „Nachbildung absolut-rechtlicher Befugnisse am Immaterialgut Daten in bilateralen Verhältnissen zwischen Vertragsparteien“[65] bezeichnet. Der Vertrag sollte also die dem Inhaber zustehenden und nicht zustehenden Verwendungsarten so konkret und umfassend wie möglich definieren und zuweisen.[66] Möglich ist natürlich auch die Einräumung einer Mitberechtigung mehrerer. In der Literatur wird hierfür teilweise auf die Gemeinschaft nach Bruchteilen rekurriert, um § 743 Abs. 2 BGB zur Anwendung bringen zu können.[67]

Zumeist sind solche Vereinbarungen nicht Gegenstand eines eigenständigen Vertrags, sondern nur Bestandteil oder Ausgangspunkt einer Datennutzungs- oder -übertragungsvereinbarung. In solchen Fällen kann die originäre Zuweisung schon die Nutzungs- und Verwertungsberechtigungen der Beteiligten vorwegnehmen oder einleiten. Die Übergänge sind fließend. Erzeugen beispielsweise mehrere Unternehmen gemeinsam bestimmte Datensätze, so kann einem von ihnen die zukünftige Kontrolle über die Daten ermöglicht und den anderen nur Rechte auf Zugang, Nutzung oder finanzielle Kompensation eingeräumt werden.[68]

Es ist aber noch einmal zu betonen, dass durch solche Inhaberschaftsvereinbarungen eventuell bestehende gesetzliche Rechte Dritter weder begründet, noch beschränkt oder zum Erlöschen gebracht werden können.[69] Wenn die fraglichen Daten allein oder in ihrer Gesamtheit einem der o.g. dinglichen Schutzrechte unterfallen, kann die „Inhaberschafts“vereinbarung ggf. aber die Zuordnung dieser Rechtspositionen bestimmen. Voraussetzung ist jeweils, dass insoweit eine vertragliche Vereinbarung überhaupt möglich ist und nicht eine zwingende Anordnung durch das Gesetz aufgrund objektiver Umstände erfolgt. So wird bspw. der Datenbankhersteller nach § 87a Abs. 2 UrhG allein durch die Vornahme der wesentlichen Investition, also objektiv bestimmt und kann daher allein durch die Verteilung der unterschiedlichen Beiträge mehrerer beeinflusst werden.[70] Eine entsprechende „Inhaberschafts“vereinbarung dürfte aber regelmäßig als Übertragung des Herstellerrechts (nach §§ 398, 413 BGB) auszulegen sein.[71]

In der Praxis kommt es durchaus häufig vor, dass solche Inhaberschaftsvereinbarungen klauselmäßig mit einem Erwerbsvertrag über die datenproduzierende Sache kombiniert werden. So haben die Hersteller von Fahrzeugen oder Maschinen ein durchaus nachvollziehbares Interesse an den von ihren Produkten erzeugten Rohdaten. Sie sind deshalb versucht, sich in den Allgemeinen Geschäftsbedingungen ausschließliche

---

64 *Berger,* ZGE/IPJ 9 (2017), 340, 351; *Apel*, Beck´sche Online-Formulare IT- und Datenrecht, 9. Ed. 1.5.2021, Form. 3.1 Anm. 1-11 Rn. 1 mwN; s.a. *Kraul,* GRUR-Prax 2019, 478, 479.

65 *Kraul,* GRUR-Prax 2019, 478, 479.

66 *Kraul,* GRUR-Prax 2019, 478, 479; *Stender-Vorwachs/Steege*, NJOZ 2018, 1361, 1363; *Kraus, D*atenlizenzverträge, in: Taeger (Hrsg.), Internet der Dinge, 2015, S. 537, 544.

67 *Kornmeier/Baranowski,* BB 2019, 1219, 1224 f.; s.a. *Ensthaler,* NJW 2016, 3473, 3477 f.

68 Vgl. *Berger,* ZGE/IPJ 9 (2017), 340, 351.

69 *Stender-Vorwachs/Steege*, NJOZ 2018, 1361, 1363; *Kraus,* Datenlizenzverträge, in: Taeger (Hrsg.), Internet der Dinge, 2015, S. 537, 544 f.

70 A.A. offenbar *Assion/Mackert,* PinG 2016, 161.

71 Vgl. Wandtke/Bullinger/*Hermes,* 5. Aufl. 2019, UrhG § 87a Rn. 134.

Zugriffs- und Nutzungsrechte hinsichtlich dieser Daten einzuräumen. Für deren praktische Wirksamkeit werden die Hersteller zudem technische Zugriffs- und Nutzungsschranken sowie automatische Datenübertragungen in die Produkte implementieren.[72] Dass solche Vereinbarungen gegen § 433 Abs. 1 S. 1 BGB iVm § 903 BGB und ggf. § 307 Abs. 1 S. 1 BGB verstoßen,[73] ist jedoch nicht ausgemacht. Nicht jede Nutzungsbeschränkung ist ein Verstoß gegen § 903 BGB: Der Erwerber eines Films auf einer DVD darf diese z.B. auch nicht gewerblich vorführen oder verleihen. Und technische Einschränkungen des Produkts mögen einen Sachmangel darstellen, das Eigentum bezieht sich aber auf das Produkt „so wie es ist". Der Maßstab der Sach- und Rechtsmängelhaftung dürfte hier auch passender sein, als ein Rekurs auf ein abstraktes Vertragsleitbild[74]. In Betracht kommt aber durchaus, dass solche Klauseln angesichts des sonstigen Vertragstexts überraschend sind.[75]

bb) Datenkauf und Datenmiete

Ist die Datenherrschaft nicht unklar, sondern begehrt ein Unternehmen Zugang zu Daten, die einem anderen Unternehmen „gehören", dann handelt es sich um einen „Datenzugangsverschaffungsvertrag". Wie bereits ausgeführt wurde, sollte sich die Zugangsberechtigung auf alle drei Betrachtungsebenen der Daten erstrecken, um eine rechtssichere Grundlage für die eigentlich erstrebte Datennutzung zu bieten.

Wie im analogen Bereich, kommen hierfür auch im digitalen Datenrecht mehrere Vertragstypen in Betracht. In der Literatur werden vor allem kauf- und mietähnliche Gestaltungen einander gegenübergestellt;[76] freilich bleibt die Abgrenzung dieser beiden Typen oftmals im Dunkeln. Teilweise wird zudem auf den Begriff der Datenlizenz abgestellt.

Ferner ist zu erwägen, ob die weithin als Datenmiete eingeordneten Verträge nicht besser dem Pachtrecht zuzuschlagen sind.[77] Im Unterschied zur Miete gewährt die Pacht dem Pächter neben den Nutzungsvorteilen des Pachtgegenstands auch den Genuss von dessen Früchten iSv § 99 BGB, vgl. § 581 Abs. 1 S. 1 BGB. Zwar werden Lizenzverträge schon herkömmlich als Pachtverträge eingeordnet,[78] mangels eigener Körperlichkeit sind Daten jedoch jedenfalls keine Sachfrüchte iSv § 99 Abs. 1 BGB[79] und für die Rechtspacht fehlt es an einem Recht (s.o. ■III. 3.■). Will man über die Anwendung des Pachtrechts aber eigentlich nur über § 581 Abs. 2 BGB zu den sonst auf körperliche Gegenstände begrenzten Vorschriften des Mietrechts kommen,[80] dann stellt die Anwendung derselben den besseren Weg dar. Hierfür bedarf es seit der Umsetzung der Digitale-Inhalte-Richtlinie 2019/770 wegen § 548a BGB auch keiner

---

72 Vgl. *Kühling/Sackmann,* ZD 2020, 24, 28.

73 So *Fritzsche,* FS Harte-Bavendamm, 2020, S. 33, 41 f.

74 An der Existenz eines relevanten Leitbilds zweifelt z.B. *Kraus,* Datenlizenzverträge, in: Taeger (Hrsg.), Internet der Dinge, 2015, S. 537, 545.

75 *Fritzsche,* FS Harte-Bavendamm, 2020, S. 33, 44 f.

76 *Berger,* ZGE/IPJ 9 (2017), 340, 351.

77 Z.B. *Schicker,* in Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, Kap. 7.2 Rn. 5.

78 MüKoBGB/*Harke,* 8. Aufl. 2020, BGB § 581 Rn. 27; Staudinger/*Schaub* (2018) Vorbem zu § 581, Rn. 44, 83 ff.

79 BeckOGK/*Mössner,* 1.3.2021, BGB § 99 Rn. 10.2 mwN.

80 *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung, 2012, Rn. 506 ff., 524 ff.; im Anschluss daran *Rank-Haedler,* Daten als Leistungsgegenstand, in: Specht-Riehmenschneider/Werry/Werry (Hrsg.), Datenrecht in der Digitalisierung, 2020, S. 489 Rn. 38.

Analogie mehr. Danach sind die Vorschriften über die Miete von Sachen auf die Miete digitaler Produkte, also digitaler Inhalte oder digitaler Dienstleistungen (vgl. § 327 Abs. 1 S. 1 BGB), entsprechend anzuwenden. Digitale Inhalte sind dabei gemäß § 327 Abs. 2 S. 1 BGB Daten, die in digitaler Form erstellt und bereitgestellt werden, also auch solche Daten, wie sie hier von Interesse sind.

Die bereits erwähnte Schwierigkeit, Kauf und Miete/Pacht voneinander abzugrenzen, folgt dabei aus dem Fehlen einer dinglichen Rechtsposition, die der „Veräußerer" dem „Erwerber" verschaffen kann. Weil nach dem oben Gesagten die Datennutzung eigentlich frei ist, stellen der faktische Datenzugang und seine Kontrolle den eigentlichen „Verfügungsgegenstand" eines Datenkaufs dar. Ebenso wird für die erlaubte Nutzung auf Basis eines Datennutzungsvertrags ein faktischer Zugang zu den Daten verschafft. In beiden Konstellationen „erwirbt" der Erwerber nur einen schuldrechtlichen Anspruch auf ein bestimmtes faktisches Handeln.[81]

Der Unterschied liegt also allein im Umfang der durch den Zugang verschafften Nutzungsmöglichkeiten. Wann dieser eher einem Kauf oder einer Miete vergleichbar ist, muss also von anderen Kriterien abhängen. Zumeist wird darauf abgestellt, ob die zu verschaffende Datennutzungsberechtigung dauerhaft und endgültig oder nur vorübergehender Natur ist.[82] Fraglich ist aber, ob daneben ein Kauf voraussetzt, dass der Erwerber eine ausschließliche Nutzungsberechtigung erwirbt und/oder dass der Veräußerer seine Hoheits- und Nutzungsrechte vollständig aufgibt, also gleichsam translativ überträgt.[83] Auch ließe sich fragen, ob ein „Kauf" den Erwerb einer weiterveräußerungsfähigen Position voraussetzt oder vorschreibt.[84]

Ein Kaufvertrag iSv § 433 BGB liegt jedenfalls vor, wenn ein Datenträger übereignet und übergeben werden soll. Einigkeit besteht auch darin, dass Daten an sich gemäß § 453 Abs. 1 BGB verkauft werden können.[85] Macht dann aber eine vertraglich vereinbarte nur vorübergehende Nutzungsberechtigung an den darauf enthaltenen Daten den Vertrag zu einem Mietvertrag oder stellt sich die Nutzungsbeschränkung als Mangel der Kaufsache dar oder handelt es sich gar um zwei voneinander zu trennende Verträge oder zumindest um einen gemischt-typischen Vertrag? Vieles spricht daher für eine im Ausgangspunkt getrennte Betrachtung der drei Daten-Ebenen. Zugleich sind hiermit schon einige der regelungsbedürftigen Einzelfragen skizziert.

Im Ergebnis braucht daher die Absenz einer zu erwerbenden dinglichen Rechtsposition nicht überbetont zu werden. Entscheidend ist, ob in der Zusammenschau der gewollten Rechte und Pflichten der Parteien dem Erwerber eine vollrechtsähnliche

---

81 *Steinrötter,* FS Taeger, 2020, S. 491, 509; *Markendorf,* ZD 2018, 409, 410.

82 So wohl *Schicker,* in Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, Kap. 7.2 Rn. 18; *Krätzschmar,* Rechtliche Anforderungen an Datenaustauschverträge, in: Taeger (Hrsg.), Internet der Dinge, 2015, S. 753, 759; *Berger,* ZGE/IPJ 9 (2017), 340, 351; s.a. *Schur,* Die Lizenzierung von Daten, 2020, S. 170 („befristete oder inhaltlich beschränkte Nutzung").

83 So wohl *Hennemann,* RDi 2021, 61 Rn. 12.

84 So z.B. *Berger,* ZGE/IPJ 9 (2017), 340, 351.

85 Z.B. Jauernig/*Berger*, BGB, 18. Aufl. 2021, BGB § 453 Rn. 11; *Krätzschmar,* Rechtliche Anforderungen an Datenaustauschverträge, in: Taeger (Hrsg.), Internet der Dinge, 2015, S. 753, 759; *Hoeren/Pinelli,* JZ 2020, 879, 880; *Peschel/Rockstroh,* MMR 2014, 571, 576; *Schicker,* in Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, Kap. 7.2 Rn. 18; *Stender-Vorwachs/Steege*, NJOZ 2018, 1361, 1363 (wenngleich ablehnend zur Bezeichnung als „Kauf"); in der Sache auch *Sattler,* in: Schmidt-Kessel/Grimm (Hrsg.), Telematiktarife & Co., 2018, S. 1, 11.

Position, also die „Dateninhaberschaft“, übertragen werden soll,[86] oder ob im Gegensatz dazu nur einzelne Nutzungsberechtigungen (ggf. aber auch dauerhaft) eingeräumt werden sollen. Im ersten Fall ähnelt der Vertrag einem Kauf, im zweiten einer Miete.

cc) Unentgeltliche Verträge, Tauschverträge

Schließlich kann zwischen entgeltlichen und unentgeltlichen Verträgen und nach der Art der Gegenleistung unterschieden werden. Ohne Gegenleistung wird der Kauf zur Schenkung, die Miete zur Leihe; bei einer Gegenleistung, die nicht in Geld oder personenbezogenen Daten besteht, handelt es sich um Elemente eines Tauschvertrags. Im Folgenden sollen diese Verträge aber ausgeklammert bleiben.

b) Übergreifende Fragen

Zuerst sollen die Punkte untersucht werden, die für alle Arten von Datenverträgen gleichermaßen relevant sind.

aa) Faktische Herrschaft und Kontrolle als Vertragsgegenstand

Zuvörderst sollten die Datenverträge deutlich zum Ausdruck bringen, ob und welche dinglichen Rechtspositionen eingeräumt werden sollen und dass sich der Verschaffungswille der Beteiligten vor allem auf die faktische Herrschaft und Kontrolle über die fraglichen Daten bezieht. Kommt es den Parteien – wie regelmäßig – nicht auf die Einräumung einer bestimmten, dinglichen Rechtsposition an, so muss der Vertrag das widerspiegeln, um Zweifel an den Rechtsfolgen des Fehlens einer solchen gesicherten Position auszuräumen. Anderenfalls kommt Unmöglichkeit gemäß § 275 Abs. 1 BGB oder ein Wegfall der Geschäftsgrundlage nach § 313 BGB in Betracht.[87]

Für den Fall, dass doch dingliche Ausschließlichkeitsrechte beim Veräußerer vorhanden sein können, bietet sich zum einen eine spezifische Zusatzklausel an.[88] Zum anderen könnte der Vertrag gleich „alle bestehenden und übertragbaren Positionen“ erfassen.[89] Auch wenn letzteres dogmatische Schärfe vermissen lässt, bringt die Formulierung doch zum Ausdruck, dass eben übertragen werden soll, was übertragen werden kann. Auch im Übrigen sollte der Vertragswortlaut auf den Begriff der „Verfügung“ verzichten, solange nicht tatsächlich dingliche Rechte übertragen werden.[90]

Anwendungen. *Vor dem Hintergrund der o.g. Anwendungsbeispiele wird damit deutlich, dass vor allem die technische Datensouveränität über die Nutzungsmöglichkeiten von Daten entscheidet. Bei der* ***internen Datennutzung*** *wird genügt also schon das Innehaben der Daten; eine Ausschließungsmöglichkeit ist keine Voraussetzung für die rechtmäßige Verwendung der Daten.*

---

[86] In diesem Sinne wohl auch *Hennemann,* RDi 2021, 61 Rn. 10.

[87] *Schicker,* in Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, Kap. 7.2 Rn. 3.

[88] *Schicker,* in Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, Kap. 7.2 Rn. 18 f.

[89] Z.B. *Sommer/Morsbach,* in Cichon/Sommer/Morsbach, BeckFormular IT-Recht, 5. Aufl. 2020, S. 774, 776 (sub § 6).

[90] Missverständlich daher *Kühling/Sackmann,* ZD 2020, 24, 27. Gegen den Euphemismus des „Nutzungsrechts“ lässt sich dogmatisch nichts einwenden, weil durch den Vertrag zusätzlich zur faktischen, rechtlich freigestellten Nutzungsmöglichkeit ein relatives Datenverwertungsrecht begründet wird.

*Bei **interner Datenherkunft** sind mit Ausnahme datenschutzrechtlicher Regulierungen für personenbezogene oder personenbeziehbare Daten damit kaum besondere rechtlichen Schranken zu berücksichtigen. So kann Unternehmen A die im eigenen Produktionsbetrieb generierten Daten z.B. zur Optimierung von Produktionsabläufen usw. („Product Maintenance") nutzen und dazu in jeglicher Form verarbeiten. Entsprechend stellt sich die Sachlage im Falle einer externen Nutzung interner Daten dar (Unternehmen B und C), bei der die Daten z.B. an externe Datennutzer übertragen (Datenkauf, Datenmiete) werden oder Daten in einem gemeinsamen Pool mit einer oder mehr Parteien geteilt werden.*

*Etwas komplexer gestalten sich die Überlegungen im Kontext der internen Datennutzung, wenn die Daten aus **externen Datenquellen** stammen. Hier lassen technische Instrumente den Zugriff auf die Daten des Fahrzeugs (Unternehmen D) oder der Anlagen (Unternehmen E) zu, sodass die Nutzungsmöglichkeit grundsätzlich gegeben ist. Auch die Übertragung der Daten mittels geeigneter Übertragungstechnologien ist problemlos möglich. Allerdings sollte der Abruf der externen Daten des Fahrzeugs oder der Anlagen nicht stillschweigend nach Übereignung der Sache erfolgen, weil hierin eine Vertragsverletzung des Kaufvertrags und damit ein Mangel – mit den entsprechenden Konsequenzen und Möglichkeiten des Käufers vom Vertrag zurückzutreten oder Schadensersatz zu verlangen (§ 437 BGB) – liegen kann.*

bb) Kategorien von Daten

Von übergreifender Bedeutung ist zudem die genaue Beschreibung der vertragsgegenständlichen Daten. Mit einem Datenvertrag will eine Partei einer anderen Zugang zu bestimmten Daten verschaffen. Die Parteien müssen sich dabei zuerst darüber verständigen, welche Qualitäten die Daten haben sollen. Die benötigten Eigenschaften richten sich vorrangig nach der bezweckten Verwendung durch den Erwerber, nicht immer aber kann und will der Veräußerer jede dieser Eigenschaften sicherstellen.

Insoweit wird u.a. danach unterschieden, welchen Grad der Strukturierung, der Aktualität oder der Aggregation Datensätze haben.[91] Strukturierte Daten sind nach einem vorgegebenen inneren Format geordnet und geben damit Relationen klarer wieder als unstrukturierte Daten; sie sind aber oftmals weniger flexibel einsetzbar. Semistrukturierte Daten sind ihrerseits mit Metadaten verknüpft, die eine Analyse der Daten erleichtern sollen. Die Aktualität der Daten (also der Informationen) wiederum kann von einem beliebigen Punkt in der Vergangenheit bis zu Echtzeit-Datenflüssen reichen. Aggregierte Daten fassen eine Mehrzahl von Einzeldaten zu einem einzigen Wert zusammen. Die Aggregation kann sich dabei ihrerseits auf eine Vielzahl unterschiedlicher Eigenschaften beziehen, also auf die Datenherkunft, alle Informationen über eine Person/Maschine, eine Information über viele Personen/Maschinen usw. Zudem können Daten unmittelbar erhoben und unbearbeitet sein, immer häufiger werden Daten aber auch nachträglich aufbereitet, um die Datenqualität (dazu noch sogleich) zu verbessern. Über die Analyse von Roh- oder Primärdaten gewonnene Informationen werden wiederum als abgeleitete Daten bezeichnet.[92] Auch darüber hinaus kann die Art der Erhebung die Daten kennzeichnen.[93]

---

91 *Schweitzer,* GRUR 2019, 569, 571; s.a. *Krätzschmar,* Rechtliche Anforderungen an Datenaustauschverträge, in: Taeger (Hrsg.), Internet der Dinge, 2015, S. 753, 754.

92 *Schweitzer,* GRUR 2019, 569, 571.

93 *Krätzschmar,* Rechtliche Anforderungen an Datenaustauschverträge, in: Taeger (Hrsg.), Internet der Dinge, 2015, S. 753, 764.

cc) Datenqualität

Die Festlegung der Datenkategorien lässt sich schon als Teil der Fixierung der Qualitätsmerkmale der vertragsgegenständlichen Daten ansehen. Die Datenqualität ist wesentlicher Bezugspunkt der Hauptleistungspflicht und damit Katalysator einer eventuellen vertraglichen Haftung.[94] Gleichzeitig bestimmen oftmals schon die technischen Rahmenbedingungen, welche Zusagen diesbezüglich gemacht werden können.

Neben den o.g. Datenkategorien sollte die Vereinbarung alle drei Ebenen berücksichtigen und daher konkrete Aussagen auch zur Beschaffenheit eventueller Datenträger, vor allem aber zu Dateiformaten und Rechten Dritter enthalten. Außerdem sind Absprachen bezüglich Aktualität, Umfang, Aussagegehalt, Verfügbarkeit oder der Herkunft der Daten sinnvoll. Der Datenqualität lassen sich auch Vereinbarungen darüber zuordnen, wer die erhobenen Daten auf welche Weise prüft. Nachträgliche Veränderungen oder die Vollständigkeit der Daten ließen sich unter das Stichwort der Richtigkeit fassen.[95]

Für all das haben sich bislang noch keine Marktstandards etabliert, so dass es an einem objektiven Erwartungshorizont fehlt. Solange die Fallgestaltungen zudem noch vielseitig und wenig vergleichbar sind, ist daher die individuelle Vereinbarung zwischen den Parteien besonders von Bedeutung. Zumeist dürfte danach ein bestimmter wirtschaftlicher Wert der Daten vom Veräußerer nicht garantiert werden; eine entsprechende Klarstellung kann sich jedoch anbieten.

Objektive Qualitätskriterien könnten aber beispielsweise die Genauigkeit der ermöglichten Vorhersagemodelle sein, oder die Robustheit gegen vorsätzliche Datenveränderungen oder andere spezifische Eigenschaften einer auf Basis der Daten trainierten KI. Sehr strenge Anforderungen formuliert insofern beispielsweise Art. 10 Abs. 3, Abs. 4 E-KI-VO. Ob diese überhaupt erfüllbar sind, ist freilich zweifelhaft.[96] Als Alternative dazu können die Parteien auch an einen subjektiven Bemühensmaßstab denken. Solche Anstrengungen sind jedoch oftmals nicht nachprüfbar und bringen schnell beide Parteien in Beweisnöte.

Ob darüber hinaus Toleranzen für Abweichungen sinnvoll sind, hängt vom Einzelfall ab.[97] Bei einer kaufähnlichen Dateninhaberschaftsvereinbarung dürfte eine prozentuale oder absolute Untergrenze für die Verwertbarkeit der Daten zu den vom Erwerber gesetzten Zwecken üblich sein.[98] Eine 100%ige Übereinstimmung mit den Qualitätskriterien wiederum dürfte für den Veräußerer zumeist nicht sicherzustellen sein. Die Toleranzen sollten aber jedenfalls individuell im Hinblick auf die einzelnen Kriterien vereinbart werden. Bei mietähnlichen Datenlizenzen ist vor allem zu regeln, ob und wie die Aktualität der Daten auch auf Dauer sichergestellt werden soll.

---

[94] Zur schwierigen Abgrenzung von Qualitätsvereinbarung und Inhalt der Hauptleistungspflicht *Hennemann,* RDi 2021, 61 Rn. 17; am Beispiel des Garantievertrags MüKoBGB/*Wurmnest,* 8. Aufl. 2019, § 307 Rn. 16.

[95] Krit. *Hoeren/Pinelli,* JZ 2020, 879, 882, weil Big-Data-Analysen nur Wahrscheinlichkeiten und Korrelationen aufdeckten.

[96] Krit. auch *Ebers/Hoch/Rosenkranz/Ruschemeier/Steinrötter,* J 2021, 4, 589, 595.

[97] *Krätzschmar,* Rechtliche Anforderungen an Datenaustauschverträge, in: Taeger (Hrsg.), Internet der Dinge, 2015, S. 753, 761; *Assion/Mackert,* PinG 2016, 161, 163.

[98] Vgl. *Feldmann/Höppner,* in: Moos, Datennutzungs- und Datenschutzverträge, 2014, S. 339, 343.

dd) Bestimmtheit und Bestimmbarkeit der geschuldeten Daten

Um den Vertragsgegenstand möglichst genau zu kennzeichnen, müssen die erfassten Datenbestände definiert werden. Dafür können die Parteien zuerst abstrakt oder konkret auf den Inhalt der Daten Bezug nehmen. Gerade bei dynamischen Datenbeständen kann sich eine abgrenzende Beschreibung jedoch schwierig gestalten.[99] Hier könnte besser auf den Erhebungsvorgang abgestellt werden.[100]

Hoeren/Pinelli haben zudem darauf hingewiesen, dass eine solche Umschreibung von vertragsgegenständlichen Daten dem Maßstab des § 253 Abs. 2 Nr. 2 ZPO nicht genügen könnte. Hier könnten Prüfsummen helfen, jedoch müsste dann der Anspruchsinhaber schon vorher die Prüfsumme der Daten kennen, was letztlich auf ein Kennen der selbst Daten hinausläuft.[101] Außerdem helfen Prüfsummen nur bei einem feststehenden Datenbestand. Aktualisierungen, Ergänzungen oder gar im Fluss befindliche Datensammlungen könnten von vornherein nicht erfasst werden.

Die mangelnde Bestimmtheit macht einen Datennutzungsvertrag nicht unwirksam, seine (gerichtliche) Durchsetzung würde gleichwohl erschwert. Für einvernehmliche Regelungen könnte es sich anbieten, die erfassten Daten nach ihrer Zuordnung zu und auf den Datenträgern zu definieren. Damit hat dann zwar der Leistungsschuldner die Bestimmung des Umfangs der Daten faktisch in der Hand. Die richtige Klassifizierung der Daten wird jedoch durch den Vertragsgegenstand mit vorgegeben und ist daher ihrerseits vertragliche Pflicht.

Leichter dürfte sich die Menge der Daten umschreiben lassen.[102] Hier kann auf die Anzahl der Datensätze oder den Speicherplatz abgestellt werden; beides ist freilich seinerseits im Einzelnen definitionsbedürftig.

ee) Abgrenzung zum Datenschutzrecht / zu personenbezogenen Daten

Zur semantischen Qualität der Daten gehört insbesondere deren Personenbezug iSv Art. 4 Nr. 1 DSGVO, der die Anwendbarkeit des Datenschutzrechts zur Folge hat. Auch wenn Gegenstand des Datenvertrags nach Vorstellung der Parteien gerade Daten ohne Personenbezug sind, sollte doch für diesen Fall Vorsorge getroffen werden.

Die Parteien sollten sich daher jedenfalls über die Risiken des weitreichenden Begriffs des Personenbezugs verständigen. Wie oben erläutert ist auch im unternehmerischen Kontext nicht ausgeschlossen, dass eine Datenverarbeitung doch an die Vorgaben der DSGVO gebunden ist. Bestehen dann rechtliche Schranken für die Verarbeitung, kann dies als Mangel qualifizieren. Sind die Hürden unüberwindbar, kann Unmöglichkeit iSv § 275 Abs. 1 BGB vorliegen. Schließlich kann der ganze Vertrag nach § 134 BGB nichtig sein.[103] Es ist an den Parteien, sich zu überlegen, ob deshalb Gewährleistungsrechte insoweit ausgeschlossen sein oder gerade bestehen sollen. Möglich ist auch, Pflichten zur Anonymisierung oder Löschung zu begründen.

---

99 *Schefzig,* Die Datenlizenz, in: Taeger (Hrsg.), Internet der Dinge, 2015, S. 551, 558.

100 *Schicker,* in Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, Kap. 7.2 Rn. 22.

101 Deshalb wollen *Hoeren/Pinelli,* JZ 2020, 879, 881 die Prüfsummenverfahren auch (nur) auf die Löschung oder Rückgabe von Daten anwenden.

102 Vgl. *Krätzschmar,* Rechtliche Anforderungen an Datenaustauschverträge, in: Taeger (Hrsg.), Internet der Dinge, 2015, S. 753, 761.

103 S. OLG Frankfurt a.M., NJW-RR 2018, 887; zu einem Verstoß gegen § 203 Abs. 1 StGB z.B. BGH, NJW 1995, 2915; BGH, NJW 1991, 2955; BGH, NJW 2014, 141.

Ferner dürfte es geboten sein, zumindest die (eventuellen) datenschutzrechtlichen Verantwortungssphären abzugrenzen und ggf. Verträge nach Art. 28 Abs. 3 DSGVO oder Art. 26 Abs. 1, 2 DSGVO abzuschließen. Soweit die Parteien eigene Verarbeitungsinteressen an den Daten haben, sollte ihnen im Datenvertrag die Berechtigung zur Verarbeitung zu eigenen Zwecken eingeräumt werden. Das kann sie dann freilich zum Verantwortlichen iSv Art. 4 Nr. 7 DSGVO machen.[104] Zudem stellt die vertragliche Erlaubnis keine Ermächtigungsgrundlage gegenüber den Betroffenen dar; hierfür bedarf es eines eigenständigen Tatbestands.[105] Nach überwiegender Ansicht bedarf es freilich für die Weitergabe der Daten an einen Auftragsverarbeiter keiner eigenständigen Rechtfertigung, weil hierin keine Verarbeitung iSv Art. 4 Nr. 2 DSGVO liegt.[106]

ff) Gewährleistungsrechte

Die Vereinbarung von bestimmten Qualitäten der Daten wirft die Frage nach Inhalt und Grenzen einer diesbezüglichen Gewährleistung und Haftung des Datengebers auf. Unabhängig vom Vertragstyp lösen Schlechtleistungen des Datengebers gesetzliche Gewährleistungsrechte aus, falls diese nicht wirksam ausgeschlossen wurden.

a) Gesetzliche Gewährleistungsrechte

Den hier interessierenden Fallbeispielen liegen sämtlich B2B-Konstellationen zugrunde. Dementsprechend sollen im Folgenden Fragen des Verbraucherschutzes ausgeklammert werden. Damit finden insbesondere die §§ 312 ff. BGB sowie die §§ 327 ff. BGB keine Anwendung. Gerade letztere können aber durchaus Anregungen für regelungsbedürftige Sachfragen im Zusammenhang mit Datennutzungsverträgen bereithalten.

Beim Datenkauf finden auf die hier interessierenden B2B-Verträge nach § 453 Abs. 1 S. 1 BGB die §§ 434 ff. BGB Anwendung. Im Falle von Sach- oder Rechtsmängeln werden danach die in § 437 BGB genannten Rechte des Datenkäufers ausgelöst. Wird die Qualität von Daten zwischen den Parteien erschöpfend vertraglich geregelt, stellen nur Abweichungen von diesem Maßstab einen Mangel iSv § 434 Abs. 1 S. 1 BGB dar und ist ein Rückgriff auf eventuelle objektive Kriterien ausgeschlossen.[107] Unabhängig davon findet § 377 HGB Anwendung, weil Daten als Waren iSd §§ 373 ff. HGB anzusehen sind.[108] Für die Untersuchungsobliegenheit des § 377 Abs. 1 HGB muss aber gerade nur unternommen werden, was „nach ordnungsmäßigem Geschäftsgange tunlich ist".

Auch bei mietähnlichen Verträgen ist gemäß § 536 Abs. 1 S. 1, Abs. 3 BGB entscheidend auf die Vereinbarung der Parteien über den Verwendungszweck der Daten abzustellen.[109] Im Grundsatz ist zudem Bezugspunkt der Mangelfreiheit auch hier die im Zeitpunkt des Vertragsschlusses zu erwartende Beschaffenheit. Verändern sich also

---

104 Vgl. EuGH v. 5.6.2018 – C-210/16, ECLI:EU:C:2018:388 – *Wirtschaftsakademie Schleswig-Holstein*.

105 Im Hinblick auf KI-Training z.B. *Piltz/Zwerschke,* in Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, Kap. 8.5 Rn. 17 ff.

106 *Golland,* ZD 2020, 397, 400 mwN; a.A. BeckOK DatenschutzR/*Spoerr,* 38. Ed. 1.11.2021, DS-GVO Art. 28 Rn. 29 ff.

107 Vgl. § 434 Abs. 3 S. 1 BGB.

108 MüKoHGB/*Grunewald,* 5. Aufl. 2021, HGB Vor § 373 Rn. 3; OLG München BeckRS 2009, 27252.

109 Allg. BeckOGK/*Bieder,* 1.4.2021, § 536 Rn. 30.

später die üblichen Anforderungen an einzelne Qualitäten von Daten, so hat dies auf den Umfang der vom Datengeber geschuldeten Leistung keine Auswirkung.[110]

Die meisten der oben genannten Qualitäten sind sicherlich den Sachmängeln zuzuschlagen sein. Daneben dürften Nutzungsbeschränkungen aufgrund entgegenstehender Rechte Dritter als Rechtsmängel einzuordnen sein. Solche Rechte Dritter können sich auf allen drei Ebenen ergeben, dürften sich jedoch zumeist auf den gedanklichen Inhalt der Daten und damit die Semantik beziehen. Hierunter fällt z.B., dass die Daten rechtswidrig erlangt wurden und deshalb deliktsrechtliche oder strafrechtliche Nutzungseinschränkungen drohen.[111]

Von besonderer Bedeutung sind zudem Beschränkungen, die sich aus dem Schutz von personenbezogenen Daten ergeben. Zwar wird hier davon ausgegangen, dass die lizenzierten Daten keinen Personenbezug aufweisen, jedoch sollte im Vertrag auch an dieser Stelle entsprechend Vorsorge getroffen werden. Unbeschadet eventueller Marktstandards oder konkreter Absprachen der Parteien kann der Erwerber im Regelfall erwarten, dass er die erhaltenen Daten auch rechtmäßig zu den vertraglich vorgesehenen Zwecken verarbeiten kann. Weitere Nutzungsmöglichkeiten muss der Datengeber nicht sicherstellen. Soweit der Datengeber die Verarbeitungsfähigkeit der Daten schuldet, muss er im Rahmen der Nacherfüllungs- oder der Erhaltungspflicht einen ausreichenden datenschutzrechtlichen Erlaubnistatbestand herbeiführen. Kann oder will er das nicht, kommen Schadensersatzansprüche in Betracht.

b) Vertragliches Haftungsregime

Die gesetzliche Rechtslage vermag über den subjektiven Mangel die Vereinbarungen der Parteien im Grundsatz gut abzubilden und sich konkreten Absprachen anzupassen. Gleichwohl kann es aus Sicht der Parteien erstrebenswert sein, das gesetzliche Haftungsregime durch ein eigenständiges vertragsrechtliches zu ersetzen.[112] Das verstößt im Unternehmerverkehr nicht gegen § 307 Abs. 1 BGB.[113] Auch aus einer Indizwirkung[114] von § 309 Nr. 8 lit. b) BGB ergibt sich nicht Gegenteiliges. Denn Daten mögen sich zwar nicht abnutzen, sondern allenfalls inhaltlich oder im Format veralten,[115] sie können aber durchaus einem alterungsbedingten Fehlerrisiko unterliegen, das regelmäßig durch einen entsprechenden Preisabschlag berücksichtigt wird,[116] und sind daher nicht „neu“ iS dieser Vorschrift.[117]

Auch die inhaltlich anzustellenden Erwägungen unterscheiden sich nicht von anderen komplexen Transaktionsverträgen und sollen hier deshalb nicht nachgebildet werden. Kern des individuellen Gewährleistungsregimes sollten konkret vereinbarte

---

110 Allg. BeckOGK/*Bieder,* 1.4.2021, § 536 Rn. 31.

111 *Assion/Mackert,* PinG 2016, 161, 163.

112 Auch die Praxis orientiert sich an den üblichen Mustern und verweist entweder auf die gesetzlichen Gewährleistungsrechte oder installiert (ergänzend) ein eigenständiges Gewährleistungsregime, vgl. z.B. § 9 des Musters bei Weitnauer/Mueller-Stöffen/*Imhof,* Beck’sches Formularbuch IT-Recht, 5. Aufl. 2020, H.6.

113 BeckOGK/*Fehrenbach*, 1.12.2021, BGB § 307 Gewährleistungsklausel Rn. 63, mit Einzelerläuterungen in den Rn 64 ff..

114 Zu ihr z.B. BeckOGK/*Richters/Friesen,* 1.10.2021, BGB § 310 Rn. 52 ff.

115 Das betonen *Hoeren/Pinelli,* JZ 2020, 879, 883.

116 Darauf stellt zu Recht ab BeckOK BGB/*Becker,* 59. Ed. 1.5.2021, BGB § 309 Nr. 8 Rn. 23.

117 Zur Einbeziehung von Daten in den Sachbegriff des § 309 Nr. 8 lit. b) BGB siehe BeckOGK/*Weiler,* 1.9.2021, BGB § 309 Nr. 8 Rn. 96; MüKoBGB/W*urmnest,* 8. Aufl. 2019, § 309 Nr. 8 Rn. 14.

Service Level im Hinblick auf alle drei Ebenen des Datenrechts sein. Für den Erwerber besonders wichtige Eigenschaften sollten dabei verschuldensunabhängig garantiert werden.[118] Hier bieten sich Vertragsstrafen an, weil der Nachweis eines Schadens oft nur schwer zu führen sein wird.[119] Andererseits sollten die Datenlieferanten auch die spätere Verwendung der Daten im Blick haben, weil sonst Schadensersatzansprüche drohen auch im Hinblick auf mit diesen oder aufgrund dieser Daten erbrachten Dienstleistungen des Datenerwerbers.[120]

c) Einzelheiten zum „Datenkauf"

Neben diesen allgemeinen Fragen erscheinen in einem Dateninhaberschaftsübertragsvertrag, oder kurz Datenkauf, spezielle Punkte regelungsbedürftig.

aa) Inhalt der erworbenen Positionen

Vorrangig ist durch die Parteien zu bestimmen, welche Rechte, Berechtigungen und sonstige rechtlichen oder tatsächlichen Positionen an den Erwerber übertragen werden sollen. Für eine dem Kauf vergleichbare Übertragung einer dem Vollrecht entsprechenden Dateninhaberschaft muss der Erwerber neben einem einfachen Zugang zu den Daten zumindest das Recht auf wirtschaftliche Verwertung derselben erhalten. Konstitutiv dürfte auch die Gewährung des Rechts sein, über die Integrität der Daten zu disponieren, also deren Veränderung, Ergänzung oder Löschung zu bestimmen und diese auch tatsächlich zu kontrollieren. Soweit dingliche Rechte an den einzelnen Daten oder ihren Aggregationen bestehen, müssen diese natürlich soweit möglich übertragen werden. Ferner geht die Literatur davon aus, dass der Erwerber die Daten auch frei weiterübertragen können muss.[121]

Unklar ist, ob darüber hinaus der Veräußerer seine Herrschaftsposition an den vertragsgegenständlichen Daten vollständig aufgeben muss, weil nur dann die Dateninhaberschaft vergleichbar dem Eigentum nach § 433 Abs. 1 S. 1 BGB translativ auf den Erwerber übertragen wird.[122] Wirtschaftlich dürfte damit eher die Frage der erstrebten Exklusivität der Datenherrschaft und der daraus folgenden Nutzungsmöglichkeiten im Hinblick auf den Veräußerer und Dritte angesprochen sein.[123] Rechtlich stellt sich gleichsam die Frage, ob ein Datenkauf nach §§ 453, 433 BGB eher dem Verkauf einer Kopie oder dem Verkauf des Originals vergleichbar sein muss. Während beim Sachkauf die Übertragung des Eigentums an einer Kopie grundsätzlich genügt, behandelt das Urheberrecht diesen Fall als Einräumung eines Nutzungsrechts und damit als „Lizenzierung". Beim Zusammentreffen von Sache und Urheberrecht bestimmt die Reichweite des Erschöpfungsgrundsatzes, welches Rechtsregime sich durchsetzt.[124]

---

118 *Assion/Mackert,* PinG 2016, 161, 163.

119 *Fries/Scheufen,* MMR 2019, 721, 724; *Krätzschmar,* Rechtliche Anforderungen an Datenaustauschverträge, in: Taeger (Hrsg.), Internet der Dinge, 2015, S. 753, 765; krit. dazu *Hoeren/Pinelli,* JZ 2020, 879, 882.

120 *Assion/Mackert,* PinG 2016, 161, 163.

121 *Berger,* ZGE/IPJ 9 (2017), 340, 351.

122 Zum Erfordernis der Aufgabe jeder Einwirkungsmöglichkeit auf die Sache BGH NJW 1996, 2643, 2655.

123 Für bestimmte, einzelne Verwendungsmöglichkeiten können auch sog. Rücklizenzen eingerichtet werden.

124 Bei verkörperten Werken gilt § 17 Abs. 2 UrhG, bei unverkörperten Werken ist zu unterscheiden: Software unterliegt der Erschöpfung nach § 69c Nr. 3 S. 2 UrhG, andere Werke

Aus der Perspektive der Vertragsgestaltung ist zu ergänzen, dass sich auch aus eventuellen Beschaffenheitsvereinbarungen ein Rückschluss auf die geschuldete Leistung ergeben kann. Wenn beispielsweise Freiheit von Rechten Dritter geschuldet wird,[125] so ist das ersichtlich an §§ 433 Abs. 1 S. 2, 435 BGB angelehnt.[126] Wenn aber gleichzeitig der Veräußerer nicht gewährleistet, dass der Erwerber Ausschließlichkeitsrechte erwirbt,[127] dann zählt jedenfalls die Übertragung oder Begründung ebensolcher nicht zum Pflichtenprogramm des Veräußerers.

bb) Durchführung von Löschungspflichten

Ist danach eine translative Übertragung notwendig, schuldet der Veräußerer zusätzlich zur Übertragung der Daten auch die vollständige Löschung aller Kopien auf den ihm zugänglichen Datenträgern.[128] Wie ein solches Löschen rechtssicher festgestellt und ggf. nachgewiesen werden kann, ist umstritten. Die Praxis der Einholung notarieller Testate[129] wird zunehmend in Zweifel gezogen.[130]

Auch ist zweifelhaft, wie eine Löschung technisch umgesetzt werden kann. Die Informationen ganzer Speichermedien können durchaus noch physisch so gelöscht werden, dass sie nur mit großem Aufwand oder sehr geringer Erfolgswahrscheinlichkeit wiederhergestellt werden können. Demgegenüber können Daten mit im Verhältnis zur Größe des Speichermediums abnehmendem Umfang immer wahrscheinlicher wiederhergestellt werden.[131] Erschwert wird dies noch, wenn die Daten auf virtuellen Zusammenschlüssen mehrerer physischer Datenspeicher verteilt gelagert und deshalb ggf. automatisch zur Sicherheit kopiert werden.[132] Kommt es dem Erwerber gerade auf die restlose Löschung der Daten an,[133] sollte daher ein bestimmtes Maß an geringer Wahrscheinlichkeit dafür definiert werden, dass der Veräußerer (ggf. unter Zuhilfenahme Dritter) die Daten wieder herstellen kann.[134] Möglich ist auch, die anzuwendenden Löschungsmethoden konkret zu vereinbaren und in der Vertragsurkunde festzuschreiben. Angesichts der genannten Schwierigkeiten empfehlen sich schließlich auch insoweit spezielle Sanktionsmechanismen.

---

nicht; vgl. EuGH v. 19.12.2019 – C-263/18, ECLI:EU:C:2019:1111 – *Tom Kabinet*; EuGH v. 3.7.2012 – C-128/11, ECLI:EU:C:2012:407 – *UsedSoft*; aus der Literatur z.B. *Schneider,* WRP 2021, 293 ff.; *Hilty,* GRUR 2018, 865 ff.

125 Z.B. § 4 Abs. 5 des Musters bei Weitnauer/Mueller-Stöffen/*Imhof,* Beck'sches Formularbuch IT-Recht, 5. Aufl. 2020, H.6.

126 S.a. § 327g BGB n.F.

127 Z.B. § 4 Abs. 6 S. 2 des Musters bei Weitnauer/Mueller-Stöffen/*Imhof,* Beck'sches Formularbuch IT-Recht, 5. Aufl. 2020, H.6.

128 Vgl. EuGH v. 3.7.2012 – C-128/11, ECLI:EU:C:2012:407 – *UsedSoft* zum softwarerechtlichen Erschöpfungsgrundsatz.

129 Dazu z.B. *Seitz,* Gebrauchte Softwarelizenzen, 2010, S. 229 Fn. 580.

130 *Hoeren/Pinelli,* JZ 2020, 879, 881.

131 Eingehend *Hunzinger,* Das Löschen im Datenschutzrecht, 2018, S. 118 ff.

132 *Hunzinger,* Das Löschen im Datenschutzrecht, 2018, S. 144 ff.

133 Für einen solchen Fall s. z.B. *Sommer/Morsbach,* in Cichon/Sommer/Morsbach (Hrsg.), BeckFormular IT-Recht, 5. Aufl. 2020, S. 774, 777 und 779.

134 In diesem Sinne für das Datenschutzrecht *Hunzinger,* Das Löschen im Datenschutzrecht, 2018, S. 260 ff.

cc) Bereitstellung der Daten

Nach alledem ist die einzige Handlung, zu der sich der Veräußerer stets verpflichtet, die Verschaffung der Datenhoheit an den Erwerber in Form eines Realakts.[135] Sie ist das Äquivalent zur nach § 433 Abs. 1 S. 1 BGB geschuldeten Übergabe der Sache; mangels Sachqualität der Daten findet bei nichtkörperlichen Übertragungen jedoch keine „Übergabe" iSe Besitzwechsels/Besitzübertragung[136] statt.[137] Zunehmend wird daher auf den im BGB bislang nicht vorbelasteten Begriff der „Bereitstellung" abgestellt.[138] Dies hat den Vorteil, dass keine unzutreffenden dogmatischen Assoziationen geweckt werden. Die nötigen Abgrenzungen kann der Begriff selbst eben deshalb jedoch nicht liefern, wie schon die Definition des § 327b Abs. 3 BGB n.F. zeigt. Danach ist ein digitaler Inhalt bereitgestellt, wenn er dem Erwerber „zur Verfügung gestellt oder zugänglich gemacht worden ist". Letztlich kommt es danach also doch wieder auf den „Zugang" oder das ebenso unscharfe „zur Verfügung stellen"[139] an.

Die Vertragsparteien sind daher gut beraten, selbst zu definieren, auf welchem technischen Weg der Zugang und die Übertragung der tatsächlichen Kontrolle bewerkstelligt werden soll.[140] Heutzutage wird hierfür zumindest ein Downloadangebot nötig sein, welches zumindest durch eine Zwei-Faktor-Authentifizierung geschützt ist. Die Vereinbarung sollte sich ferner auf Datenformat oder Kompatibilitätsanforderung, den Zugangszeitraum und die Tragung der entsprechenden Kosten beziehen.

dd) Gefahrübergang und Risikosphären

Wie bei anderen Übertragungsverträgen sollten die Parteien auch hier ihre jeweiligen Risikosphären voneinander abgrenzen und insbesondere die Transportgefahr ausdrücklich zuweisen. Für auf Datenträgern verkörperte und übertragene Daten kann hier an § 446 BGB angeknüpft werden. Beim internetbasierten Abruf muss vor allem die Tätigkeit der eingeschalteten Internet-Provider zugeordnet werden.[141] Es bietet sich – wie stets – an, möglichst exakt und konkret zu definieren.[142] Gleichzeitig sollte bedacht werden, dass es hierbei nicht nur um die Zurechnung von Gehilfenverhalten geht, sondern auch das Risiko von Zufall oder dem Handeln Dritter erfasst ist.

ee) Umfang der Rückgewährpflicht

Auch eine eventuell geschuldete Rückgewähr von bereitgestellten Daten erfolgt unterschiedlich in Abhängigkeit vom vereinbarten Vertrag. Bestand die

---

135 *Steinrötter,* FS Taeger, 2020, S. 491, 509; *Berger,* ZGE 9 (2017) 340, 350; *Zech,* Data as a tradeable commodity, in: de Franceschi (Ed.), European Contract Law and the Digital Market, 2016, S. 51, 60.

136 Zur Kritik an diesem Begriff MüKoBGB/*Schäfer,* 8. Aufl. 2020, BGB § 854 Rn. 50.

137 Missverständlich daher BGH NJW 1996, 2159, 2161 („der tatsächliche Besitz der Kundendaten").

138 *Hennemann,* RDi 2021, 61 Rn. 12; *Schicker,* in Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, Kap. 7.2 Rn. 22.

139 S.a. § 5 Abs. 1 des Musters bei Weitnauer/Mueller-Stöffen/*Imhof,* Beck'sches Formularbuch IT-Recht, 5. Aufl. 2020, H.6; s. aber Abs. 2 ebenda, der für den Gefahrübergang auf eine „Übergabe der Daten" abstellt.

140 *Kraus,* Datenlizenzverträge, in: Taeger (Hrsg.), Internet der Dinge, 2015, S. 537, 547.

141 *Krätzschmar,* Rechtliche Anforderungen an Datenaustauschverträge, in: Taeger (Hrsg.), Internet der Dinge, 2015, S. 753, 763.

142 *Peschel/Rockstroh,* MMR 2014, 571, 575 mit dem Beispiel „WAN-Ausgang des vom Operation-Center verwendeten Routers".

Hauptleistungspflicht in einer „Entäußerung“ der Daten, müssen diese vom Erwerber zurückübertragen werden. In allen Konstellationen sind die erhaltenen Daten dann zu löschen, was dieselben Probleme wie bei der entsprechenden Primärleistungspflicht aufwirft (siehe oben ■III.4.c.bb.■). Noch grundsätzlicher kann die Sinnhaftigkeit einer Rückgewähr zweifelhaft sein aufgrund eines zwischendurch eingetretenen Verlusts an Aktualität und Exklusivität oder wenn die Daten schon vom Erwerber verwendet wurden;[143] dabei sollte allerdings die Einschätzung der Parteien respektiert werden.

Bei Konstellationen, in denen die Daten zwischenzeitlich vom Erwerber verändert oder ergänzt wurden, ergeben sich noch weitere Probleme. Zuerst fragt sich, was zurück zu gewähren ist, wenn der Erwerber keine Kopie der ursprünglich erworbenen Daten mehr hat. Zudem ist zu überlegen, in welchem Umfang sich die korrespondierende Löschungspflicht auch auf den modifizierten Datensatz erstreckt. Dahingehend ließe sich erwägen, dass die veränderten Datensätze Nutzungen iSv § 346 Abs. 1 Hs. 2 BGB sind. Damit ist auf § 100 BGB verwiesen, der die Gebrauchsvorteile erfasst, aber nicht solche durch Verbrauch der Sache oder dafür erhaltene Surrogate. Soweit der ursprüngliche Datensatz nicht mehr erzeugt werden kann, wird demnach die Rückgewährpflicht aus § 346 Abs. 1 BGB unmöglich iSv § 275 Abs. 1 BGB und regelmäßig § 346 Abs. 2 BGB ausgelöst. Dann wird jedoch nur Wertersatz geschuldet und gerade nicht die Rückabwicklung des Datenkaufvertrags erreicht. Die Parteien sollten also klarstellen, bis zu welchem Grad an Weiterverarbeitung bzw. Veränderung der Ursprungsdaten, diese dennoch Gegenstand eines Rückgewähranspruchs oder jedenfalls eines Löschungsanspruchs sein können.

Von der Pflicht zur Rückgewähr der Nutzungen nach § 346 Abs. 1 Hs. 2 BGB sind aber jedenfalls nicht die aus den Daten entwickelten Produkte und Dienstleistungen erfasst.[144] Wie bei Maschinen, deren Produkte keine Früchte darstellen,[145] sind auch nicht die aus einer Datennutzung gewonnen oder verbesserten Produkte deren Nutzungen. Allenfalls die aus der Nutzung der Daten gewonnenen weiteren Erkenntnisse und Informationen („Daten“) könnte man als solche Gebrauchsvorteile ansehen, wenngleich das schon für die von Maschinen erzeugten Daten überwiegend verneint wird.[146] Unabhängig davon dürfte die Herausgabe aber regelmäßig nach § 346 Abs. 2 Nr. 3 BGB ausgeschlossen sein. Dann kommt allenfalls ein entsprechender Wertersatzanspruch in Betracht, dessen Berechnung besonderen Schwierigkeiten unterliegt[147]; es bietet sich angesichts von § 346 Abs. 2 S. 2 Hs. 1 BGB ggf. an, den einzelnen Qualitätsmerkmalen konkrete Gegenleistungswerte zuzuordnen.

Anwendungen. *Vor dem Hintergrund unserer Anwendungsbeispiele wird damit deutlich, dass in erster Linie für die Konstellationen B und D ein Datenkauf relevant wird, während für die Anwendungsbeispiele C und E eher die Datenmiete genutzt werden sollte.*

Bei der ***externen Datennutzung*** *ist der Unternehmensfokus direkt auf die Veräußerung der Daten gerichtet. So räumt der Datenverkäufer (B) dem Datenkäufer die geschuldeten Rechte an den gekauften Daten ein. Je nach Verwendungszweck lassen sich*

---

143 *Sommer/Morsbach,* in Cichon/Sommer/Morsbach, BeckFormular IT-Recht, 5. Aufl. 2020, S. 774, 785.

144 So aber *Hoeren/Pinelli,* JZ 2020, 879, 881.

145 BeckOGK/*Mössner,* 1.3.2021, BGB § 99 Rn. 5.4

146 Vgl. BeckOGK/*Mössner,* 1.3.2021, BGB § 99 Rn. 10.2.

147 *Hoeren/Pinelli,* JZ 2020, 879, 881.

die Daten an einen Käufer (exklusiv) oder mehrere Käufer übertragen (nicht-exklusiv). Etwa bei Verkehrs- und Umweltdaten (z.B. Daten zu Feinstaubbelastung, Emissionen, Anzahl der Fahrzeuge in einem Zeitabschnitt oder geografischen Raum) lassen sich in der Regel viele Anwendungsfälle (z.B. Apps, Immobilienwerte) zur Nutzung der Daten finden, sodass ein Mehrfachverkauf der Daten sinnvoll erscheint. Im Datenkontext ist die Exklusivität allerdings nicht vordergründig, weil nicht die Daten, sondern vielmehr die Datenauswertung für den Käufer in der Regel wertstiftend ist. Gerade vor dem Hintergrund der besonderen Eigenschaft der Nicht-Rivalität von Daten, sollten zudem aus ökonomischer Sicht so viele Nutzer wie möglich die Daten verwenden, sodass Exklusivität nur bedingt sinnvoll erscheint (z.B. im Falle prohibitiver Datenerhebungskosten).

*Bei der **internen Datennutzung** sind die Daten die Schlüsselressource für den Unternehmenserfolg, insbesondere wenn für datengetriebene Geschäftsmodelle der Unternehmenserfolg direkt mit der Datenverfügbarkeit und -auswertung zusammenhängt. So ist für den Produktentwickler (D) oft eine Vielzahl unterschiedlicher Datenquellen Ausgangspunkt für das eigene Produkt. Der Hersteller eines autonomen Fahrzeugs greift u.a. auf große Datensätze zur Bilderkennung zurück, um Gefahrenquellen und -potenziale zu erkennen und hierauf zu reagieren. Auch für den Produktentwickler ist die Exklusivität der Daten nicht besonders wichtig, sondern sind vor allem die Datenqualität und -quantität für den Trainingsprozess und die Inbetriebnahme elementar. Für den Plattformbetreiber (F) als Intermediär zwischen u.a. Käufer und Verkäufer von Daten spielt der konkrete Kaufprozess nur bedingt eine Rolle. Insbesondere dann, wenn die Datenübertragung über die Plattform abgewickelt wird oder der Plattformbetreiber Vertragsmuster bereitstellt, könnten nichtsdestotrotz auch hier Gewährleistungspflichten zu berücksichtigen sein.*

d) Einzelheiten zur „Datenmiete“

Auch ein Vertrag zur Bereitstellung von Nutzungsmöglichkeiten an Daten hat zum Ziel, die Verwertung des Gutes „Daten“ einvernehmlich zu regeln.[148] Hierbei dürften ebenso einige Punkte besonders zu beachten sein.

aa) Konstitutive Nutzungsbeschränkungen

Vor dem Hintergrund der oben gemachten Ausführungen, dass eine Nutzung von nicht-personenbezogenen Daten grundsätzlich keiner Berechtigung, sondern nur einer faktischen Kontrolle bedarf, muss jeder Datenmietvertrag neben der Bereitstellung von Daten zu einem oder mehreren bestimmten Zwecken – ausdrücklich oder konkludent – auch einen Ausschluss der Nutzungsberechtigung zu anderen als diesen Zwecken enthalten. Mangels genereller ausschließlicher Rechtsposition kann der Mieter nämlich nur vertraglich an bestimmten Nutzungsweisen (einschließlich der Weiterveräußerung) der Daten gehindert werden; zu Allem, was er faktisch kann, ist der Mieter auch „dinglich“ berechtigt. Fehlt es an solchen Beschränkungen, handelt es sich deshalb doch um einen Datenkauf – ggf. zu einem bestimmten Zweck. Ob die unterschiedlichen Berechtigungen und Nicht-Berechtigungen dann positiv oder negativ formuliert werden, ist zu Recht als Stilfrage bezeichnet worden.[149]

---

148 *Schefzig,* Die Datenlizenz, in: Taeger (Hrsg.), Internet der Dinge, 2015, S. 551, 556.

149 Vgl. *Schefzig,* Die Datenlizenz, in: Taeger (Hrsg.), Internet der Dinge, 2015, S. 551, 558.

Die Nutzungsbeschränkungen können zudem durch tatsächliche Schutzmaßnahmen vom Vermieter kontrolliert und durchgesetzt werden. Idealerweise erfolgt die geschuldete Bereitstellung der Daten also nicht durch Verschaffung einer umfassenden Kontrolle über dieselben, sondern nur durch Gewährung eines technisch limitierten Zugangs zu den Daten. Ggf. erfolgt die erlaubte Datennutzung sogar ausschließlich im Herrschaftsbereich des Vermieters, d.h. insbesondere als Cloud-Lösung.

bb) Pflicht zur Bereitstellung

Hauptleistungspflicht des Vermieters ist deshalb auch hier die Bereitstellung von Daten – beschränkt auf bestimmte Nutzungszwecke. Dieser Begriff passt neben den o.a. Kaufverträgen auch für die hiesigen Mietkonstellationen, weil er nicht nach Dauer oder Umfang differenziert und nur an den tatsächlichen Zugang abstellt. Die Parteien sind frei zu vereinbaren, welches Maß an technisch/faktischer Kontrolle des Mieters über die Daten erreicht werden muss.

cc) Typisierung

Die Datenmiete wird zumeist als Lizenzvertrag bezeichnet. Für die Typisierung eines Datennutzungsvertrags ist hierdurch freilich nicht viel gewonnen, weil es an einer gesetzlichen Ausformung eines allgemeinen Lizenzvertrags fehlt. Eben deshalb ist die Verwendung dieses Begriffs aber auch unschädlich. Zudem wird er trotz aller Versuche zur seiner Spezifizierung in der Literatur[150] oftmals beliebig verwendet.

In der Sache orientiert sich die Literatur für die Datenlizenz zumeist an spezifischen immaterialgüterrechtlichen Lizenzverträgen und ihren gesetzlichen Ausformungen, insbesondere an urheberrechtlichen Nutzungsrechtseinräumungen.[151] Angesichts der Absenz gesetzlich bestimmter oder sonst konturierter, absoluter Rechte an Daten trägt dieser Vergleich wohl nicht.[152] Es liegt näher, sich an Verträgen zu orientieren, die ebenso ungeschützte Vermögensgegenstände „lizensieren". Hierfür bieten sich deshalb die praktisch erprobten, sog. „Know-How-Verträge" bzw. „Know-How-Lizenzen" an, mit denen schon bislang rechtlich nicht spezifisch geschütztes Wissen übertragen wurde.[153]

dd) Umfang und Inhalt der Berechtigungen

Auch hinsichtlich des Umfangs der einzuräumenden Nutzungsberechtigungen haben die Parteien weitgehend freie Hand. Sie sollten aber sicherstellen, dass der Mieter/Lizenznehmer ausreichende Berechtigungen hinsichtlich aller drei Betrachtungsebenen erhält. Welche Mindestberechtigungen das sind, hängt zum einen von eventuellen Schutzrechten an der Semantik und zum anderen von der tatsächlichen Ausgestaltung der Datenbereitstellung ab. Sind die Daten als Datenbank oder Geschäftsgeheimnis geschützt, so muss die Vereinbarung auch entsprechende Nutzungsrechte einräumen. Bei Datenbanken ist dann § 87e UrhG zu beachten, wonach der Datenbankhersteller die Vervielfältigung, Verbreitung oder öffentliche Wiedergabe von nach Art und Umfang unwesentlichen Teilen der Datenbank nicht vertraglich beschränken kann, soweit sie

---

150 Z.B. *McGuire,* Die Lizenz, 2012, S. 267 ff.; *Pfaff/Nagel* in: Pfaff/Osterrieth (Hrsg.), Lizenzverträge, 4. Aufl. 2018, A. Allgemeiner Teil, Rn. 13 ff.; s.a. *Obergfell/Hauck,* in: dies. (Hrsg.), Lizenzvertragsrecht, 2. Aufl. 2020, 1. Kap. Rn. 1 ff.

151 Vgl. *Hennemann,* RDi 2021, 61 Rn. 26 f.

152 *Hoeren/Pinelli,* JZ 2020, 879, 880.

153 Ebenso *Schur,* Die Lizenzierung von Daten, 2020, S. 156.

einer normalen Auswertung der Datenbank nicht zuwiderlaufen und die berechtigten Interessen des Datenbankherstellers nicht unzumutbar beeinträchtigen. Letzteres dürfte bei Trainingsdatenbeständen, die nicht zur Veröffentlichung bestimmt sind, jedoch regelmäßig nicht erfüllt sein. Bei Geschäftsgeheimnissen wiederum ordnet § 2 Abs. 3 GeschGehG ausdrücklich an, dass eine rechtsgeschäftliche Gestattung den Lizenznehmer berechtigt, das Geschäftsgeheimnis zu erlangen, zu nutzen oder offenzulegen.

Jedenfalls bietet es sich an, die notwendigen Berechtigungen strukturiert im Hinblick auf den jeweiligen Vertragszweck zu erarbeiten. Hierfür werden unterschiedliche Systematisierungen erwogen. *Zech* schlägt drei Kategorien vor: Zugang, Nutzung und Integritätshoheit.[154] Der Zugang zu den Daten ist danach nur ein Aspekt der notwendigen Berechtigungen. Unter die eigentlich beabsichtigte Nutzung sollen sich dann Vervielfältigung, Verbreitung und Analyse/Auswertung der Daten fassen lassen; zur Integritätshoheit gehört vor allem die Frage der Veränderung und Löschung der Daten oder ihres Inhalts. Gerade wenn Daten zum Training verwendet werden sollen, bedarf es der Befugnis, diese ggf. auch zu verändern, mit anderen Daten zu kombinieren und zu analysieren.[155] In Konzernstrukturen kann auch die Weitergabe an konzernangehörige Dritte notwendig werden. Alternativ wird erwogen, sich am Datenschutzrecht und damit heute an der Aufzählung von Art. 4 Nr. 2 DSGVO zu orientieren.[156] Danach sollten die Parteien über „das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“ der Daten sprechen. Wichtig ist in jedem Falle die Klärung der Berechtigungen der Beteiligten hinsichtlich der Analyseergebnisse; hieran können sämtliche Vertragspartner ein berechtigtes Interesse haben.

Die einzelnen Nutzungshandlungen können zudem an bestimmte Zwecke gebunden werden.[157] Diese Bindung ist freilich rein schuldrechtlicher Natur, deswegen aber auch nur von den allgemeinen Schranken begrenzt. Vergleichbar dem Urheberrecht kann sich daher der Dateninhaber die intensivere Datennutzung auch intensiver bezahlen lassen.

a) Exklusivität

Ebenso wie bei anderen immateriellen Gütern kann auch die Vergabe von Nutzungsberechtigungen an Daten in unterschiedlichem Maße exklusiv erfolgen. Aus den Spezialmaterien sind die Begriffe der „einfachen“ und „ausschließlichen“ Nutzungsrechte/Lizenzen bekannt (z.B. § 31 Abs. 2 und 3 UrhG). Danach kann die Absprache der Parteien dahingehen, dass der Lizenznehmer die Daten unter Ausschluss Dritter (also als Alleinberechtigter), neben dem Lizenzgeber oder sogar neben weiteren, ggf. später hinzutretenden Berechtigten nutzen darf.

---

154 *Zech,* CR 2015, 137, 139.

155 *Schicker,* in Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, Kap. 7.2 Rn. 20.

156 *Schefzig,* Die Datenlizenz, in: Taeger (Hrsg.), Internet der Dinge, 2015, S. 551, 559, der sich aber letztlich lieber an den Standardisierungen der Praxis ausrichten will.

157 *Schefzig,* Die Datenlizenz, in: Taeger (Hrsg.), Internet der Dinge, 2015, S. 551, 561 f.; vgl. auch *Kraus,* Datenlizenzverträge, in: Taeger (Hrsg.), Internet der Dinge, 2015, S. 537, 547

Für das notwendige Maß dieser Exklusivität existiert bislang kein normativer Standard.[158] Eine Parallele zum Urheberrecht kann nicht in allen Fällen gezogen werden, weil es gerade nicht stets der Dateninhaber ist, der besonders schutzbedürftig ist. Ein Leitbild könnte daher auch nur branchenspezifisch festgelegt werden. Die Parteien sind deshalb frei, eine ihren Interessen entsprechende Absprache zu treffen. Gerade in den hier interessierenden B2B-Konstellationen dürfte das Wettbewerbsrecht genügen, um die unangemessene Ausübung von Marktmacht zu adressieren. Zumeist werden sich die geschäftserfahrenen Parteien sich sowieso über den Grad der Exklusivität ausdrücklich verständigen, weil diese regelmäßig ein entscheidender wertbildender Faktor ist.[159]

Ob mit einer ausschließlichen Lizenz auch eine Pflicht zur Datenverwertung einhergeht, ist nicht pauschal zu beantworten. Die Ausübungspflicht dient in Verträgen zur Lizenzierung von besonderen Schutzgegenständen vor allem dem Inhaber des Schutzrechts, der die wirtschaftliche Verwertung des Schutzrechts allein dem Lizenznehmer anvertraue und deshalb insofern schutzwürdig sei.[160] Mangels einer entsprechenden Vereinbarung besteht daher nur dann eine Ausübungspflicht, wenn ein solches Verwertungsinteresse des Dateninhabers deutlich zutage getreten ist.

Anwendungen. *Vor dem Hintergrund unserer Anwendungsbeispiele wird damit deutlich, dass in erster Linie für die Konstellationen C und E die Datenmiete relevant ist. Der Plattformbetreiber spielt für die Datenmiete nur dann eine Rolle, wenn weitere Dienstleistungen, wie z.B. Cloudlösungen für Datenzugang und/oder -nutzung, zusätzlich angeboten werden. Bei Product Maintainance (A) könnte eine Datenmiete in Betracht kommen, wenn die Datenauswertung an einen externen Dritten outgesourced wird.*

Bei der ***externen Datennutzung*** *ist der Unternehmensfokus direkt auf die Veräußerung der Daten gerichtet. So räumt der Datenpool (C) die Zugangs- und Nutzungsmöglichkeit für Datenpoolmitglieder ein. In der Regel werden Datenpools hierzu mit wechselseitigen Kreuzlizenzierungen ausgestaltet, sodass alle Datenpoolbeteiligten wechselseitig die Daten des anderen nutzen können. Die Exklusivität der Datenzugangs- und Nutzungsrechte kann dabei u.a. durch die Ausgestaltung als geschlossener oder offener Pool gesteuert werden. Je nach Bedeutung des Datenzugangs für den Markteintritt (z.B. bei datengetriebenen Geschäftsmodellen) kann insbesondere die Exklusivität des geschlossenen Pools auch Gegenstand einer wettbewerbsrechtlichen Begutachtung sein, wenn der Zugang zu diesen Daten von der Wettbewerbsbehörde als „Essential Facility" eingestuft wird. Umfang und Inhalt der konkreten Nutzungsrechte sollten im Lizenzvertrag explizit berücksichtigt werden. Gerade bei z.B. Produktionsdaten sind neben Beschränkungen zu Geschäftsgeheimnissen zudem kartellrechtliche Schranken zu berücksichtigen, zumal die resultierende Markttransparenz unter Umständen kollusives Verhalten begünstigen könnte. Schließlich wäre über eine Verwertungspflicht des Anlagendienstleisters (E) nachzudenken, weil der Anlagennutzer und Bezieher der Dienstleistung sich auf die Verwendung der Daten verlässt und*

---

158 Wie hier *Schefzig,* Die Datenlizenz, in: Taeger (Hrsg.), Internet der Dinge, 2015, S. 551, 563; anders *Hennemann,* RDi 2021, 61 Rn. 27, der unter Verweis auf die Regelungen im Urhebervertragsrecht für ein Leitbild der einfachen Lizenz eintritt.

159 *Kornmeier/Baranowski,* BB 2019, 1219.

160 Vgl. *McGuire,* Die Lizenz, 2012, S. 708.

bei Nichtinformation Produktionsverzögerungen oder sogar Produktionsausfälle drohen könnten.

*Bei der **internen Datennutzung** sind die Daten die Schlüsselressource für den Unternehmenserfolg, zumal vor allem für datengetriebene Geschäftsmodelle der Unternehmenserfolg direkt mit der Datenverfügbarkeit und -auswertung zusammenhängt. So ist für den Anlagendienstleister wichtig, dass er Zugang zu möglichst aktuellen Daten (i.d.R. in Form von Echtzeitdaten) erhält, um die Datenauswertung und anschließende Dienstleistungsbereitstellung (z.B. Wartung, Austausch von Verschleißteilen, Optimierung usw.) rechtzeitig zu erbringen. Vor diesem Hintergrund ist der Kaufvertrag einer Produktionsanlage durch einen entsprechenden Lizenzvertrag zu ergänzen. Da es sich bei den Produktionsdaten um besonders sensible Daten handelt, könnte der Anlagenkäufer unter Umständen auf eine Kontrolle der eigenen Daten Wert legen. Technisch ließen sich solche Konstellationen durch entsprechende Cloudlösungen im Herrschaftsbereich des Anlagenbauers realisieren. Ein API-Zugang des Anlagenverkäufers würde gleichzeitig die Aktualität der abgerufenen Produktionsdaten sicherstellen können. Vergleichbare Lösungskonzepte wären auch im Falle eines Outsourcings der Datenauswertung beim eigenen Product Maintenance (A) denkbar.*

b) Unterlizenzierung

Mit der Exklusivität der Nutzung mag aus Sicht der Beteiligten die Frage der Unterlizenzierbarkeit der Daten eng verbunden sein. Damit ist die Frage angesprochen, ob der Lizenznehmer verpflichtet werden kann, die Datennutzung nur selbst (oder durch zugehörige Dritte) vorzunehmen. Auch hier dürfte es an einem für alle Konstellationen passenden gesetzlichen Leitbild fehlen, sind doch die denkbaren Fallgestaltungen zu vielfältig. Sieht man aber – wie hier – das Mietrecht der §§ 535 ff. BGB als gesetzliche Auffangregel an, ist nach § 540 Abs. 1 BGB die Überlassung an Dritte mangels anderweitiger Abreden ausgeschlossen. Dies scheint auch angemessen, da das Interesse des Lizenzgebers oft nicht dahin gehen dürfte, dass der Lizenznehmer nur als Zwischenhändler auftritt.[161] Andererseits ist es nicht stets so, dass der Lizenzgeber ein Interesse daran hat, dass die Daten auch ausgewertet werden. Gerade für solche Konstellationen sieht § 540 Abs. 1 BGB die Erlaubnis vor, die auch im Mietvertrag erteilt werden kann.[162]

Daher gilt das zur Exklusivität Gesagte auch hier. Wichtig ist, dass die Parteien sich hierüber verständigen und den Kreis derjenigen bestimmen, an die die Daten weitergegeben werden können. Gleiches gilt für eventuelle Zweckbeschränkungen; auch hier kommt ein „Konzernprivileg" in Betracht. Mangels gesetzlicher Grundlagen kann schließlich ein Sukzessionsschutz für die Unterlizenz nur auf Basis allseitiger Vereinbarungen entstehen.

c) Dauer und Zeiträume der Nutzung

Wichtig, wenngleich kein vertragswesentlicher Bestandteil der Einigung,[163] ist die Dauer der Nutzungsberechtigung. Die Parteien können eine einmalige oder

---

161 In diesem Sinne *Hennemann,* RDi 2021, 61 Rn. 29 iVm Rn. 23.

162 Vgl. MüKoBGB/*Bieber,* 8. Aufl. 2020, BGB § 540 Rn. 12.

163 Vgl. *Blank/Börstinghaus* in: Blank/Börstinghaus (Hrsg.), Miete, 6. Aufl. 2020, BGB § 535 Rn. 31; *Bellinghausen* in; Hannemann/Wiegner (Hrsg.), Münchener Anwaltshandbuch Mietrecht, 5. Aufl. 2019, § 8 Rn. 79 ff.; a.A. MüKoBGB/*Häublein*, 8. Aufl. 2020, BGB § 535 Rn. 3.

mehrmalige Nutzung vereinbaren. Sie können auch einen Zeitraum für die Nutzung der Daten durch den Lizenznehmer bestimmen.

Wird der Zugang zu den vertragsgegenständlichen Daten nur über einen Fernzugriff ermöglicht, sollten die Verfügbarkeitszeiten möglichst eindeutig definiert werden. Hierfür können Cloud-Verträge oder solche über andere Webservices Pate stehen. Es ist zu beachten, dass damit auch das Pflichtenprogramm bezeichnet wird und eine allzu einseitige Gestaltung als Haftungsausschluss einer entsprechenden Inhaltskontrolle unterliegen kann.

An das Ende der Nutzungsberechtigung ist zudem die Frage nach Inhalt und Umfang der Löschungspflichten des Lizenznehmers geknüpft.[164] Es stellen sich dann zuerst dieselben Probleme, wie eine physische Löschung sichergestellt werden kann.[165] Zudem ist fraglich, inwieweit sich diese Pflichten auch auf die Ergebnisse der Datenanalyse beziehen. Insoweit dürfte es auf die konkreten Umstände ankommen. Je nach Bedeutung der lizenzierten Daten für den Lizenzgeber und die Rückschlüsse, die sie auch auf Interna seines Geschäfts zulassen, kann dieser ein berechtigtes Interesse an der Verhinderung einer weiteren Nutzung haben.

d) Räumliche Schranken

Die Nutzung der Daten kann auch räumlichen Beschränkungen unterworfen werden. Solche Beschränkungen können sich pauschal auf alle eingeräumten Nutzungsmöglichkeiten beziehen oder separat für einzelne von ihnen vereinbart werden. So kann für die Datenspeicherung oder auch die Datenverarbeitung eine On-Premise-Vorgabe getroffen werden oder bestimmte Länder als Standorte ausgeschlossen werden. Wegen der potentiellen Einschlägigkeit des Datenschutzrechts kann gerade eine Beschränkung auf Staaten der Europäischen Union zweckmäßig sein; eine solche Lokalisation wird deshalb auch in AGBs nicht als problematisch angesehen.[166]

Werden für die Datenverarbeitung Dritte eingeschaltet, so muss der Lizenznehmer auch bei ihrem Einsatz sicherstellen, dass die territorialen Schranken eingehalten werden. Gerade bei der Nutzung von Clouddiensten kann hier aber schnell nicht gewünschte Staaten berührt sein.

Die territoriale Diversifizierung durch den Lizenzgeber kann sich im Grundsatz auch auf den Einsatz der Analyseergebnisse beziehen. Dann ist der Lizenznehmer verpflichtet, bestimmte Nutzungshandlungen nicht in bestimmten Staaten oder Gebieten vorzunehmen. Angesichts der berechtigten Interessen, einheitliche Produkte grenzüberschreitend anzubieten, dürften solche Beschränkungen jedoch häufig praktisch einer erfolgreichen Lizenzierung entgegenstehen.

Anerkennt man ein dingliches Ausschließlichkeitsrecht an Daten, ließe sich dieses mit dinglicher Wirkung rechtssicher nur für Deutschland lizensieren. Ob und inwieweit eine solche Zuordnung auch in anderen Staaten zu Grunde gelegt würde, bedürfte kollisionsrechtlicher Klärung.[167] Angesichts dieser Rechtsunsicherheit würden hier dennoch technische Sicherungen besonders notwendig.[168]

---

164 *Schefzig,* Die Datenlizenz, in: Taeger (Hrsg.), Internet der Dinge, 2015, S. 551, 561.
165 Dazu oben ■III.4.c.ee.■.
166 *Hennemann,* RDi 2021, 61 Rn. 30.
167 Vgl. *Steinrötter,* FS Taeger, 2020, S. 491, 499.
168 *Kühling/Sackmann,* ZD 2020, 24, 27.

Anwendungen. *Die konkrete inhaltliche Ausgestaltung eines Datenlizenzvertrages ist erneut primär für die Anwendungsbeispiele des Datenpools (C) sowie des Anlagendienstleisters (E) von elementarer Bedeutung.*

Bei der ***externen Datennutzung*** *spielen vor allem räumliche sowie teilweise inhaltliche Beschränkungen eine Rolle, wenn der Datenpool (C) etwa nicht territorial begrenzt, sondern durch ein internationales Marktumfeld charakterisiert ist. Gerade vor diesem Hintergrund könnte der Lokalisation der verwendeten Clouddienste eine wichtige Rolle zukommen, die im europäischen Raum vor dem Hintergrund stärkerer Regulierungen (gerade mit Blick auf personenbezogene Daten) eine andere inhaltliche Ausgestaltung erforderlich machen als beispielsweise im US-amerikanischen oder chinesischen Marktumfeld.*

Bei der ***internen Datennutzung*** *wird der Anlagendienstleister (A) unter Umständen Unterlizenzen für solche Wartungs- und Optimierungsarbeiten ins Auge fassen, die nicht im eigenen direkten Kernkompetenzbereich liegen. So könnten gegebenenfalls neben produktionstechnischen auch logistische Problembereiche – die neben externen Lieferanten auch den eigenen Fuhrpark betreffen können – beobachtet werden, für deren Analyse wiederum Produktionsdaten des Anlagennutzers nützlich sein könnten. Vor diesem Hintergrund könnte man in solchen Fällen auch über vertikale Datenpools entlang der Wertschöpfungskette nachdenken, bei der die Produktionsdaten in Echtzeit auf verschiedenen Ebenen der Wertschöpfung Optimierungsmöglichkeiten darstellen. Ein elementarer Baustein aus rechtsökonomischer Perspektive wird in solchen (Plattform-) Konstellationen der Datenzugang und die Interoperabilität der Daten sein, um die Datenmonetarisierung nicht nur wenigen „Gatekeepern" zu überlassen.*[169]

ee) Vertraulichkeit und Geheimhaltung

Von entscheidender Bedeutung sind Vertraulichkeitsabreden.[170] Mangels dinglichen Ausschließlichkeitsrechts an den vertragsgegenständlichen Daten kann Dritten gegenüber nur die faktische Geheimhaltung die Exklusivitätsinteressen der Beteiligten wahren. Auch ein eventueller Schutz als Geschäftsgeheimnis hängt davon ab, dass die Information nicht allgemein bekannt (§ 2 Abs. 1 lit. a GeschGehG) und Gegenstand von angemessenen Geheimhaltungsmaßnahmen ist (§ 2 Abs. 1 lit. b GeschGehG). Beides setzt vertragliche Vertraulichkeitsvereinbarungen voraus, die auch wirksam durchgeführt werden.[171] Deshalb bieten sich gerade hier Vertragsstraferegelungen an.[172]

Die Beteiligten sollten erwägen, auch die Ergebnisse der Datenanalyse in die Geheimhaltungsvereinbarung einzubeziehen.[173] Ebenso sollte im Regelfall vereinbart werden, dass die Geheimhaltungspflicht auch gegenüber Erfüllungsgehilfen oder anderen Dritten weiterzugeben ist.[174]

---

169 Ausführlicher zu Datenzugang und -interoperabilität siehe Abschnitt IV. 1.

170 *Kraul,* GRUR-Prax 2019, 478, 479; s.a. *Hennemann,* RDi 2021, 61 Rn. 6: „Kontrahieren über die punktuelle Aufhebung des Geheimnisschutzes zugunsten eines bestimmten Vertragspartners".

171 Köhler/Bornkamm/Feddersen/*Alexander*, 40. Aufl. 2022, GeschGehG § 2 Rn. 60 ff.

172 *Kornmeier/Baranowski,* BB 2019, 1219, 1221.

173 *Kraus,* Datenlizenzverträge, in: Taeger (Hrsg.), Internet der Dinge, 2015, S. 537, 547.

174 *Assion/Mackert,* PinG 2016, 161, 162.

ff) Pflichten und Haftung des Lizenznehmers

Die Parteien sollten auch die den Lizenznehmer treffenden Pflichten festlegen und die daran anknüpfenden Rechtsbehelfe des Dateninhabers ausgestalten. Als Auffangregeln kommen die allgemeinen Vorschriften zur Anwendung.

a) Gesetzliche Pflichten

Sieht man den Datennutzungsvertrag wie hier als mietähnlich an, gelten im Grundsatz die §§ 535 ff. BGB. Dort sind nur wenige Pflichten des Mieters normiert, die bei einer Datennutzung relevant werden können.

Das gilt zum einen für die Pflicht aus § 536c BGB, Mängel der Mietsache, also der Daten, dem Lizenzgeber unverzüglich anzuzeigen. Der Zweck der Vorschrift ist nämlich nach allgemeiner Ansicht darauf beschränkt, den Vermieter vor Schäden an der Mietsache zu bewahren, die durch Zuwarten entstehen. Eine Prüfpflicht ergibt sich hieraus gerade nicht.[175]

Gesetzlich normiert ist zudem die Pflicht, den Mietgegenstand zurückzugewähren, § 546 BGB. Hier stellt sich – wie oben erläutert – vor allem die Frage, wie die Daten nach Ende des Nutzungsvertrags auf Seiten des Lizenznehmers zu löschen sind.

Aus dem Mietvertrag selbst iVm § 241 Abs. 2 BGB ergeben sich schließlich Obhuts-, Schutz- und Rücksichtnahmepflichten des Lizenznehmers im Hinblick auf die vertragsgegenständlichen Daten.[176] Danach ist er zur sorgfältigen Behandlung der Daten verpflichtet und muss noch über den deliktischen Maßstab hinaus, den Lizenzgeber vor Schäden bewahren.[177]

b) Vertragliche Sorgfaltspflichten

Angesichts der unklaren Reichweite dieser gesetzlichen Pflichten, sollten die Parteien die wesentlichen Sorgfaltspflichten im Umgang mit den Daten selbst regeln. Sollen die Daten als Geschäftsgeheimnisse klassifiziert werden, setzen außerdem die von § 2 Nr. 1 lit. b GeschGehG verlangten Geheimhaltungsmaßnahmen gerade auch eine wirksame Bindung der Vertragspartner voraus.[178]

Deshalb sollten im Vertrag konkrete Maßstäbe z.B. für die Lokalisation und Aufbewahrung der Daten vereinbart werden. Essentiell sind Sicherheitsstandards für die IT-Infrastruktur, mit denen die Daten vom Lizenznehmer verwahrt und verarbeitet werden sollen.[179] Dabei können auch pauschal die ISO-Standards[180] einbezogen werden oder konkrete, abweichende Vorgaben für einzelne Sicherheitsaspekte gemacht werden. Diese können z.B. die physischen Zugangsberechtigungen und -kontrollen, die Einhaltung bestimmter Arbeitsabläufe, konkrete Schutzmechanismen (wie eine Zwei-Faktor-

---

175 BeckOK BGB/*Wiederhold,* 60. Ed. 1.11.2021, BGB § 536c Rn. 2.

176 Allg. z.B. BeckOGK/*H. Schmidt,* 1.10.2021, BGB § 535 Rn. 486 f.

177 MüKoBGB/*Häublein,* 8. Aufl. 2020, BGB § 535 Rn. 210.

178 BeckOK GeschGehG/*Fuhlrott,* 9. Ed. 15.9.2021, § 2 Rn. 32; s.a. Begr. RegE, BT-Drs. 19/4724, S. 24 f.

179 *Kraul,* GRUR-Prax 2019, 478, 479.

180 Vorgaben zur Informationssicherheit finden sich in der Normenfamilie ISO 27000 für sämtliche IT-Systeme; dazu z.B. *Weissmann,* in: Schulz (Hrsg.), Cybersicherheit, 2020, S. 73 ff. mit Darstellung der inhaltlichen Vorgaben. Vergleichbare Standards enthält der sog. „IT-Grundschutz" des Bundesamts für Sicherheit in der Informationstechnologie (BSI).

Authentifizierung),[181] oder Meldepflichten, bei Hinweisen auf eine rechtswidrige Nutzung, betreffen.

Der Lizenznehmer sollte verpflichtet werden, diese Sorgfaltspflichten auch auf ggf. beteiligte Dritte weiterzuleiten.[182] Abgesichert werden können sie mit Vertragsstrafen oder Schadenspauschalen; wobei sich ein risikobasierter Ansatz empfiehlt.[183] Zudem sollten konkrete Kontroll- und Auditrechte des Lizenzgebers erwogen werden.[184] Dessen Schutzinteressen sind dann mit den Geheimhaltungsinteressen des Lizenznehmers auszugleichen.

Anwendungen. *Vor dem Hintergrund unserer Anwendungsbeispiele wird damit deutlich, dass insbesondere für den Fall einer* ***internen Datenherkunft*** *und* ***externen Datennutzung*** *individuell vertragliche Vereinbarungen zur Haftung und spezifischen Verantwortlichkeiten (z.B. zur Datensicherung) geschlossen werden sollten. Schließlich birgt die Externalisierung interner Daten auch immer die Gefahr eines Zugriffs durch externe Dritte, die unter Umständen gar den eigentlichen Zweck der Datennutzung unmöglich machen oder zumindest erschweren. Insbesondere beim Datenkauf/-verkauf (Unternehmen B) sowie bei der Nutzung eines Datenpools (Unternehmen C) könnten Wettbewerber vom Marktzutritt u.a. auf Aftersales-Märkten, gehindert werden. Hier wird gerade vor dem Hintergrund der besonderen Charakteristika der Märkte in der Datenökonomie der gegenwärtige Rechtsrahmen nicht ausreichend sein, um Anreize zur verstärkten Nutzung, Verwertung und Teilens von Daten zu schaffen.*

IV. Rechtsökonomische Analyse

Die rechtliche Analyse zeigt, dass vor allem über vertragliche Vereinbarungen Daten ausgetauscht und verwertet werden können. Dabei reicht die rein faktische Herrschaft über die Daten aus, ohne dass ein separates Eigentumsrecht an Daten zu schaffen ist.[185] Nichtsdestotrotz stellen die besonderen Charakteristika der gegenwärtigen und zukünftigen Datenökonomie vor allem kleine und mittelständische (Handwerks-) Unternehmen vor schwerwiegende Probleme bei der Partizipation an den wirtschaftlichen Potentialen neuer datengetriebener Geschäftsmodelle.[186] So sind die Märkte der Datenökonomie zunehmend durch digitale Plattformen geprägt, woraus sich zwei zentrale Ansatzpunkte zur Schaffung eines gesetzgeberischen Anreizsystems hervorheben lassen: (1) Der Zugang zu sowie die Interoperabilität von Daten entlang der Wertschöpfungskette, (2) transaktionskostensenkende dispositive Normen, vor allem in Form von (sektorspezifischen) Musterverträgen für Daten.

---

181 *Sommer/Morsbach,* in Cichon/Sommer/Morsbach, BeckFormular IT-Recht, 5. Aufl. 2020, S. 774, 786.

182 *Schefzig,* Die Datenlizenz, in: Taeger (Hrsg.), Internet der Dinge, 2015, S. 551, 561.

183 *Schefzig,* Die Datenlizenz, in: Taeger (Hrsg.), Internet der Dinge, 2015, S. 551, 562.

184 *Schefzig,* Die Datenlizenz, in: Taeger (Hrsg.), Internet der Dinge, 2015, S. 551, 562.

185 Zu einer rechtsökonomischen Position zu einem Eigentumsrecht an Daten siehe u.a. *Rusche/Scheufen*, On (Intellectual) Property and other Legal Frameworks in the Digital Economy, IW-Report 2019, Nr. 48; *Kerber*, GRUR Int 2016, S. 989–999; *Duch-Brown/Martens/Mueller-Langer,* The Economics of Ownership, Access and Trade in Digital Data, JRC Working Papers on Digital Economy, 2017, Nr. 1.

186 *Podszun,* Handwerk in der digitalen Ökonomie: Rechtlicher Rahmen für den Zugang zu Daten, Software und Plattformen, 2021, S. 42 ff.

1. Datenzugang und -interoperabilität

Die besondere Bedeutung des Zugangs zu Daten ist vor allem vor dem Hintergrund der zunehmenden Vernetzung von Produkten, Leistungen, Kunden und Märkten zu sehen.[187] Daten werden in der digitalen Ökonomie damit zu der Schlüsselressource, die die Partizipation und den Erfolg von Unternehmen im Markt unmittelbar determiniert. Der traditionelle Marktmechanismus, in dem der Nachfrager als Schiedsrichter über Erfolg und Misserfolg im Leistungswettbewerb entscheidet, wird zunehmend durch eine zentrale, datenbasierte Steuerung verdrängt. Ohne den Zugang zu Daten und die notwendige Software verlieren leistungserbringende Unternehmen damit die Schnittstelle zum Kunden und letztlich die Geschäftsgrundlage. So werden z.B. KfZ-Werkstätten durch die zunehmende Vernetzung der Fahrzeuge (Connected Cars) keine Fahrzeuge mehr reparieren können, ohne die Fahrzeugdaten auslesen zu können, oder eine Wartung von vernetzten Geräten (z.B. im Smart Home) ohne die kompatible Software zum Datenzugang unmöglich gemacht.

Über digitale Plattformen werden die Daten zugänglich, wobei Plattformmärkte zu Ansammlung von Marktmacht tendieren und häufig durch wenige sog. Gatekeeper besetzt sind, die über den allgemeinen Zugang zur Plattform sowie die Qualität der bereitgestellten Daten entscheiden. Um im Beispiel der sog. „Connected-Cars" zu bleiben, können die Hersteller von Fahrzeugen über die technische Ausgestaltung und die Einbindung der Fahrzeugdaten in eigene Serversysteme – man spricht in diesem Zusammenhang vom sog. „Extended-Vehicle"-Konzept[188] – die exklusive Kontrolle über die Fahrzeugdaten erlangen. Durch die faktische Herrschaft über die Fahrzeugdaten kann der Hersteller auch über die Nutzung und ggf. vertragliche Weitergabe der Daten entscheiden. Die Autohersteller können ihre Marktmacht so unmittelbar auf nachgelagerte sog. Kfz-Aftermarkets verlagern, weil der Datenzugang Grundvoraussetzung für den Marktzutritt von Industrie- und Mobilitätsdienstleistern darstellen wird. Eng verbunden mit dem allgemeinen Zugang zu Daten sind Fragen zu Dateninteroperabilität sowie entsprechender Standards, zumal die zunehmende Vernetzung der Systeme und der Austausch von Daten zwischen Fahrzeugen (bzw. zwischen Geräten im Allgemeinen), Infrastruktur, Unternehmen und öffentliche Einrichtungen Kompatibilität der Hard- und Software sowie offene Datenformate voraussetzt. So ist eine zentrale Frage im „Connected-Cars"-Beispiel, ob der Zugang zu Daten über ein geschlossenes oder offenes interoperables System ausgestaltet werden sollte, in dem der Fahrzeugführer letztlich über den Datenzugang entscheiden und damit seine Schiedsrichterfunktion wieder einnehmen kann.

Eine allgemeine rechtliche Regelung zur Sicherstellung von Datenzugang und -interoperabilität ist vor dem Hintergrund der vielen Unterschiede in den Charakteristika digitaler Märkte im Detail kaum möglich. So wird auch der lang erwartete Data Act[189] – der am 23. Februar 2022 offiziell vorgestellt und frühestens 2023 in Kraft treten wird – der EU-Kommission nicht alle Marktversagensprobleme, wie Marktmacht und asymmetrische Information, lösen können. Zwar deutet der Data Act gewissermaßen einen Paradigmenwechsel an, weil er den Nutzer bzw. Anwender mehr in den Mittelpunkt

---

187 Ebenda.

188 Zur ökonomischen Analyse des Mobilitätssektors siehe *Kerber,* JIPITEC 9 (2018), 310-331 sowie *Gill/Kerber,* JIPITEC 10 (2019), 244-256.

189 Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM(2022) 68 final.

stellt, aber auch die ergänzenden Regelungen des Digital Market Acts (DMA)[190] oder des Digital Service Acts (DSA)[191] können den sektor- und branchenspezifischen Charakteristika kaum Rechnung tragen. Vielmehr können und sollten diese als Regulierung eines Mindeststandards betrachtet werden, über den hinaus sektorspezifische Einzelfallregelungen hinausgehen können. Dem entspricht es, wenn die zugunsten des Nutzers erzwungene Datentransparenz bestimmte technische Vorgaben an die Hersteller für Gestaltung und Konstruktion von digitalen Produkten voraussetzt. So verlangt Art. 3 Abs. 1 des vorgeschlagenen Data Act, dass Produkte so zu konzipieren und herzustellen sind, dass die durch ihre Verwendung erzeugten Daten dem Nutzer standardmäßig leicht, sicher und, soweit relevant und angemessen, direkt zugänglich sind.

In diesem Zusammenhang wurde vom Bundesverband der Hersteller und Importeure von Automobil-Service Ausrüstungen (ASA) im Januar 2022 eine offizielle Stellungnahme und Forderung nach der einer sektorspezifischen Regelung für das „Connected-Cars"-Beispiel veröffentlicht.[192] So stellt der ASA den gegenwärtig unzureichenden fairen Wettbewerb heraus, der durch (1) die Kontrolle der Daten durch die Hersteller mit der Folge eines Zugangs nur zu hohen Kosten, in geringem Umfang oder mit unzureichende Datenqualität, (2) vordefinierte und offenzulegende Use-Cases als Marktzutrittsbarrieren für Teilnehmer von KfZ-Aftermarkets sowie (3) eine fehlende Kundenschnittstelle durch unzureichende Kontrolle des Fahrzeughalters über die Fahrzeugdaten charakterisiert ist. Gerade die freie Wahl des Endkunden bei der Auswahl ihrer Dienstleister wird zentral hervorgehoben. Das könnte durch einen Wechsel vom „Extended-Vehicle"-Konzept hin zu einem Konzept der „Sicheren On-Board Telematik Plattform" (S-OPT) technisch und wettbewerbsgerecht umgesetzt werden.

Als ergänzendes Konzept zur Lösung der Marktversagen Marktmacht (Gatekeeper, die über Umfang, Kosten und Qualität der ausgetauschten Daten entscheiden) und asymmetrische Information (Verhandlungsmacht großer Plattformbetreiber gegenüber kleinen und mittelständischen (Handwerks-) Betrieben) wird in der Literatur vermehrt die Forderung nach sog. Datenmittlern oder Datentreuhändern diskutiert. Unter einem Datenmittler versteht man Institutionen, die Datenanbieter und -nachfrager zusammenbringen, während der Datentreuhänder als besondere Form des Datenmittlers nicht aus eigenem Interesse, sondern im Interesse eines Dritten zwischen den Marktseiten vermittelt.[193] Der Datentreuhänder tritt damit als neutrale Instanz z.B. zwischen Fahrzeughersteller, Kfz-Aftersales-Dienstleister, öffentliche Institutionen (einschließlich Forschung) und Kfz-Halter/Nutzer, um nach vordefinierten Prinzipien über die Form, den Umfang und die Kosten des Datenzugangs zu entscheiden. Für die konkrete

---

190 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über bestreitbare und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte), COM(2020) 842 final.

191 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über einen Binnenmarkt für digitale Dienste (Gesetz über digitale Dienste) und zur Änderung der Richtlinie 2000/31/EG, COM(2020) 825 final.

192 *ASA-Verband* (2022), Gleichberechtigter Zugang zum vernetzten Fahrzeug – Mobilitätsbranche fordert sektorspezifische Regelung, https://asa-verband.de/wp-content/uploads/positionspapier_gleichberechtigter_zugang_zum_vernetzten_fahrzeug_2022.pdf?x68076 [letzter Zugriff am 15.3.2022].

193 Zum Thema Datentreuhändern haben kürzlich *Louisa Specht-Riemenschneider* und *Wolfgang Kerber* eine Studie im Auftrag der Konrad-Adenauer-Stiftung (KAS) vorgelegt, siehe *Specht-Riemenschneider/Kerber,* 2022, Datentreuhänder – Gesellschaftlich nützlich, rechtlich größere Anforderungen erforderlich, KAS e.V., Analysen & Argumente, Nr. 475, Februar 2022, abrufbar unter https://www.kas.de/de/analysen-und-argumente/ [letzter Zugriff am 15.3.2022].

Ausgestaltung des Datentreuhändermodells ist allerdings hervorzuheben, dass ein „one-size-fits-all"-Modell wenig zielführend, sondern auch hier sektorspezifische Ausgestaltungsformen diskutiert werden sollten, um den Regulierungsrahmen im Einzelfall und vor dem Hintergrund der besonderen Marktcharakteristika anzupassen.

So werden im Mobilitätssektor im Wesentlichen zwei Zugangslösungen für Mobilitätsdaten diskutiert:[194] (1) eine regulatorische „fair, reasonable and non-discriminatory" (FRAND-) Lösung, die sicherstellt, dass der Datenzugang unter fairen, nicht-diskriminierenden und angemessenen Bedingungen vermittelt wird und (2) eine „On-Board-Application"-Plattform" im Sinne einer standardisierten, offenen und interoperablen Telematik (Verknüpfung von Telekommunikations- und Informationssystemen zur Generierung, Übertragung und Auswertung der Daten), die die Kontrolle über die Daten wieder an den Fahrzeughalter/-nutzer übertragen würde. Während (2) – auch im Sinne der Forderung der ASA nach einem „S-OPT"-Konzepts – das langfristige Ziel zur Lösung des Datenzugangsproblems im Mobilitäts(dienstleistungs)sektor darstellen sollte, könnte (1) eine kurzfristige Übergangslösung bieten. Die konkrete Anforderung an die technische Konstruktion, das Design und die Entwicklung von vernetzten Fahrzeugen sollte möglichst durch eine sektorspezifische Regulierung begleitet werden. Dieser spezifische Ansatz sollte ebenso verfolgt werden im Gesundheitssektor (z.B. sog. „Clean Rooms", die als neutrale Instanz unter höchsten IT-Sicherheitsstandards keinen Zugang zu den Rohdaten von Patienten, sondern höchstens zu Auswertungen zu Forschungszwecken sicherstellen) oder hinsichtlich des Persönlichkeitsschutzes im Onlinesektor (z.B. sog. „Personal Information Management Systems" [PIMS], die nicht nur die datenschutzrechtskonforme Weitergabe von persönlichen Daten im Internet, sondern auch eine Beratungsfunktion erfüllen können). Während im Gesundheitssektor das Marktversagen in einer Unternutzung der Daten besteht, kann im Onlinesektor eine Übernutzung der Daten konstatiert werden.[195] Ein „one-size-fits-all"-Modell, das beispielsweise im Data Act implementiert werden könnte, würde den spezifischen Besonderheiten und den Unterschieden eines Marktversagens durch Externalitäten nicht gerecht.

2. Datenmusterverträge

Gleichzeitig verdeutlicht die kaum vorhandene Regulierung von nicht-personenbezogenen Daten die Rolle von Verträgen, um das Teilen von Daten rechtskonform und im Sinne des Dateninhabers zu gewährleisten. Da durch den Data Act die Position des Verbrauchers gestärkt werden soll, um die Kontrolle über die eigenen Daten nicht z.B. den Herstellern, sondern den Fahrzeughaltern selbst zu überlassen, wird die Bedeutung von ergänzenden dispositiven Normen deutlich, damit sich die unterschiedliche Verhandlungsmacht und asymmetrische Informationsverteilung zwischen den Marktseiten (Dateninhaber vs. Datenempfänger) nicht in der Vertragsausgestaltung niederschlägt. Ohne entsprechende dispositive Vorschriften für Datenkauf- oder -mietverträge dürften zudem zum Teil prohibitive Transaktionskosten (u.a. durch die Konsultation eines Fachanwalts) zur individuellen Ausgestaltung der Vertragsregelung vor allem für kleine und mittelständische Firmen ohne eigene Rechtsabteilung einer Datenbewirtschaftung entgegenstehen. Dispositive Vorschriften sollen diese Transaktionskosten senken, indem den Vertragsparteien die Notwendigkeit genommen wird ihrem Willen

194 Ebenda, S. 6 f.
195 Ebenda, S. 4 f.

durch detaillierte Erklärung und Vereinbarung umfassend Ausdruck zu verleihen.[196] In diesem Zusammenhang sind vor allem Musterverträge eine transaktionskostenminimierende Möglichkeit, bei der die Vertragsparteien auf vorgefertigte Vertragswerke zurückgreifen können, ohne für die individuelle Ausgestaltung des Vertragswerkes einen Fachanwalt beauftragen zu müssen.[197]

Allerdings zeigen die bereits diskutierten Besonderheiten von digitalen Plattformmärkten, dass allgemeine Musterverträge den besonderen Charakteristika dieser Märkte nur bedingt Rechnung tragen können.[198] Unvollkommene Verträge, bei der besondere sektorspezifische Eigenschaften keine explizite Berücksichtigung finden, wären die Folge. Vor diesem Hintergrund könnten technische Hilfsmittel, wie beispielsweise ein interaktiver Vertragsgenerator, der die Auswahl von spezifischen Regelungen im Einzelfall in Form von vorgefertigten Vertragsbausteinen erlaubt, die Transaktionskosten erheblich reduzieren. Einzelne Vertragsbausteine könnten in diesem Zusammenhang eine Auswahl von verschiedensten inhaltlichen, zeitlichen und räumlichen Ausgestaltungsmöglichkeiten bieten, sowie ergänzende Vertragsbausteine auch haftungsrechtliche Besonderheiten und Verantwortlichkeiten im Einzelfall regeln. Für jeden Vertrag zwingende Bausteine könnten einen Mindeststandard definieren, über den durch Auswahl ergänzender Klauseln abgewichen werden könnte, um sektorspezifischen Besonderheiten Rechnung zu tragen. Gleichzeitig würde ein solches interaktives Werkzeug die Möglichkeit der Beratung bieten, indem erläuternder Text die Bausteine und deren rechtliche Folgen begleitet oder sogar eine künstliche Intelligenz auf individuelle Fragestellungen der Vertragspartei aufklärend reagiert. Auf diese Weise könnte in Form eines Screenings auch einem Marktversagen in Form asymmetrischer Information Rechnung getragen werden.[199]

Eine sichere und vertrauenswürdige Dateninfrastruktur zur Förderung eines Teilens und Bewirtschaftens von Daten soll das vom Bundesministerium für Wirtschaft und Energie im Jahre 2019 ins Leben gerufene Projekt GAIA-X gewährleisten.[200] Nachdem das Projekt GAIA-X auf dem Digitalgipfel 2019 vorgestellt wurde, wurde es von Vertretern aus Wirtschaft, Wissenschaft und Verwaltung aus Deutschland und Frankreich fortwährend weiterentwickelt. GAIA-X könnte dabei sowohl eine souveräne Dateninfrastruktur zur allgemeinen und sektorspezifischen Regelung eines Zugangs zu Daten bieten, als auch zur Entwicklung und Förderung dispositiver Normen durch technische Einbindung von entsprechenden interaktiven Werkzeugen zur Entwicklung (sektorspezifischer) Vertragswerke zum Teilen und Bewirtschaften von Daten.

---

196 Vgl. *Grigoleit,* Zwingendes Recht (Grundlagen), HWB-EuP, 2009, abrufbar unter https://hwb-eup2009.mpipriv.de/index.php/Zwingendes_Recht_(Grundlagen) [letzter Zugriff am 15.3.2022].

197 Vgl. z.B. das Muster für die Teilnahme an einer Industrie-4.0-Plattform unter https://www.plattform-i40.de/IP/Redaktion/DE/Downloads/Publikation/RTB%20-%20Muster-vertrag.html [letzter Zugriff am 15.3.2022].

198 *Podszun,* Handwerk in der digitalen Ökonomie: Rechtlicher Rahmen für den Zugang zu Daten, Software und Plattformen, 2021, S. 148 f.

199 Vgl. allgemein zum Screening bei asymmetrischer Information *Fritsch,* Marktversagen und Wirtschaftspolitik, 9. Aufl. 2014, S. 260 ff.

200 Weiterführend siehe https://www.bmwi.de/Redaktion/DE/Dossier/gaia-x.html [letzter Zugriff am 15.3.2022]. Für eine Einführung in GAIA-X siehe *Rusche,* Einführung in GAIA-X: Hintergrund, Ziele und Aufbau, IW-Report, im Erscheinen.

V. Fazit

Die Datenökonomie braucht ein verlässliches Daten(vertrags)recht. Mangels „Dateneigentums“ wird das „Öl“[201] der Digitalwirtschaft im Wesentlichen auf der Basis von faktischer Herrschaft und vertraglichen Vereinbarungen allokiert. Das rückt den tatsächlichen Datenzugang in den Vordergrund und betont daneben die Bedeutung einer umsichtigen und interessengerechten Vertragsgestaltung. Die vorstehende Untersuchung hat eine Reihe von regelungsbedürftigen Fragen aufgedeckt und Lösungsansätze präsentiert, sowohl für den Datenkauf als auch für die Datenmiete. Orientierung konnten die bereits erprobten Know-How-Verträge bieten, wenngleich sich aus der spezifischen Struktur von Daten auch entscheidende Besonderheiten ergeben.

Der Zugang zu Daten stellt sich auch aus ökonomischer Perspektive als zentrales Kriterium heraus. Eng hiermit verbunden sind Aspekte der Dateninteroperabilität sowie die Notwendigkeit von Standards, die kaum allgemeine, sondern vielmehr sektorspezifische Lösungsansätze und -regelungen bedürfen, um den Besonderheiten der Situation im Einzelfall gerecht zu werden. Zur Steuerung des Datenzugangs kommen neben individualvertraglichen Ansätzen vor allem gesetzliche Zugangsrechte in Betracht. Die mit einer vertraglichen Zuordnung verbundenen Transaktionskosten sollten durch (frei zugängliche) Datenmusterverträge und individualisierte technische Vertragsgeneratoren gesenkt werden. Eine solche vertrauensvolle Dateninfrastruktur könnte in Zukunft GAIA-X liefern.

Abstract: *With the digitization and networking of services, products, customers and markets, data is becoming a key resource. From a legal perspective, therefore, access to data and the contractual possibility of granting individual property-rights are coming to the fore. The first elements of a data contract law can already be identified. Various types of contracts are available for licensing non-personal data, and the tried-and-tested know-how contracts provide additional guidance.*
Access to data is also crucial from an economic perspective. This requires not only data interoperability but also uniform, albeit sector-specific standards. Besides statutory access rights, individual contractual approaches are of particular importance. Data model contracts and contract generators can reduce transaction costs.

Kontakt:
Notarassessor Dr. Frank Rosenkranz
c/o Rheinische Notarkammer
Burgmauer 53, 50667 Köln
frank.rosenkranz@gmx.de

Dr. Marc Scheufen
c/o Institut der deutschen Wirtschaft e.V.
Konrad-Adenauer-Ufer 21, 50668 Köln
scheufen@iwkoeln.de / marc.scheufen@rub.de

---

[201] Daten gelten gemeinhin als das Schmiermittel der Datenökonomie, während hiermit keine Analogie zwischen den Wirtschaftsgütern Öl und Daten hergestellt werden soll, zumal Daten durch Nicht-Rivalität und Öl durch Rivalität im Konsum charakterisiert sind.