bayme vbm

vbw




Studie

Daten als Wirtschaftsgut

Eine vbw bayme vbm Studie,
erstellt von Prof. Dirk Heckmann unter Mitwirkung von Prof. Louisa Specht

Stand: Mai 2018
www.vbw-bayern.de

Vorwort

Der Wert von Daten als Herausforderung und Chance

Daten waren in den meisten Branchen bis vor einigen Jahren oft wenig mehr als Teil des notwendigen Verwaltungsaufwands. Heute gibt es kaum einen Wirtschaftszweig, der noch keine datengetriebenen Geschäftsmodelle hervorgebracht hat. Parallel zur digitalen Transformation wächst der Wert von Daten der verschiedensten Art, und wir stehen erst am Anfang der Entwicklung.

Kaum einer würde heute noch bezweifeln, dass Daten einen Wert haben (können) und ein relevantes Wirtschaftsgut geworden sind. Den Wert von Daten und Wissen zu beziffern, fällt allen Beteiligten allerdings nach wie vor überaus schwer. Trotzdem oder vielleicht auch gerade deshalb ist bereits eine intensive Diskussion darüber entbrannt, wem welche Daten zustehen und wem die daraus generierten Werte zuzuordnen sind.

Es mag auf den ersten Blick naheliegend erscheinen, auf neue Entwicklungen mit einem neuen Rechtsrahmen zu reagieren. Die vermeintliche Ordnung wäre aber zu teuer erkauft, wenn dadurch das Neue im Keim erstickt wird und Wertschöpfung an weniger stark regulierten Standorten entsteht. Gewichtige rechtstechnische Überlegungen kommen noch dazu: jeder Eingriff in das bewährte System zieht weitreichende Folgen nach sich – in der Praxis leider oft auch ungewollte Konsequenzen mit hohem Korrekturbedarf – und sollte wohl abgewogen sein. Erster Schritt muss immer der Versuch sein, der neuen Herausforderung mit dem erprobten Instrumentarium zu begegnen.

So empfiehlt es auch der Zukunftsrat der Bayerischen Wirtschaft in *Neue Wertschöpfung durch Digitalisierung – Analyse und Handlungsempfehlungen*: Gesetzgeberischer Aktionismus ist zu vermeiden, vertragliche Lösungen sind einem neuen „Dateneigentum“ klar vorzuziehen. Für die dazu notwendige Einordnung in unser heutiges Rechtssystem soll unsere vorliegende Studie einen Beitrag leisten.

Bertram Brossardt
22. Mai 2018

Inhalt

Hinweis

1 Einleitung

Daten als Produktionsfaktor im digitalen Zeitalter

Nach der betriebswirtschaftlichen Definition werden als Wirtschaftsgüter sämtliche Güter bezeichnet, die in einem Arbeitsprozess für die Leistungserstellung notwendig sind. Neben Sachgütern können hierunter auch Dienstleistungen sowie bestimmte Rechte und Informationen fallen.[1] Dass Daten mitunter bedeutende Wirtschaftsgüter darstellen können, beschäftigt nicht nur seit der Diskussion um das automatisierte Fahren beinahe täglich die Tagespresse, sondern ist auch Gegenstand zahlreicher Fachbeiträge und Studien, darunter etwa aus der Informatik, der Rechtswissenschaft oder der Betriebswirtschaftslehre.[2] Selbst die Rechtsprechung bezeichnet inzwischen sogar nicht nur im insolvenzrechtlichen Kontext[3] explizit Daten als Wirtschaftsgut und geht überdies davon aus, dass die zunehmende wirtschaftliche Bedeutung von Datenerhebungen auch auf die Entwicklung des Verständnisses des Datenschutzrechts Einfluss nimmt.[4] Schließlich impliziert auch bereits der Gesetzgeber mit dem Vorhandensein der Vorschrift des § 29 Bundesdatenschutzgesetz (BDSG), dass es einen Markt für – personenbezogene – Daten geben soll.[5] § 29 BDSG gestattet unter bestimmten Voraussetzungen das geschäftsmäßige Erheben, Speichern, Verändern oder Nutzen von Daten zum Zweck der Übermittlung, insbesondere wenn dies der Werbung, der Tätigkeit von Auskunfteien oder dem Adresshandel dient. Daten können also im digitalen Zeitalter als eine Art Produktionsfaktor angesehen werden.[6]

Ausgehend von der grundsätzlichen und damit zugleich essentiellen Frage, was unter dem Begriff „Daten“ zu verstehen ist, gibt es einige zentrale rechtliche Anknüpfungspunkte, die nachfolgend beleuchtet werden: Wer darf auf Daten, die in verschiedenen Prozessen, z. B. beim autonomen Fahren, anfallen, zugreifen? Welchen Wert haben Daten? Wie ist die Bezahlung mit Daten rechtlich einzuordnen? Was gibt es aus datenschutz- und IT-sicherheitsrechtlicher Sicht beim Umgang mit Daten zu beachten? Zudem stellt sich die Frage, ob jeder Verstoß gegen Datenschutzvorschriften zugleich einen Vertragsverstoß darstellt und anders herum. Diese und weitere Fragen werden im Anschluss in einer Darstellung bestehender Querbeziehungen zwischen den unterschiedlichen Regelungsmaterien aufgeworfen.

Ziel dieser Studie ist es, die teils sehr komplexen juristischen Diskussionen zu strukturieren und für den unternehmerischen Gebrauch verständlich aufzubereiten.

---

[1] http://www.unternehmerlexikon.de/wirtschaftsgut/, zuletzt abgerufen am 13.06.2017.
[2] Vgl. etwa KPMG/bitkom, Mit Daten Werte schaffen, Report 2016, https://home.kpmg.com/de/de/home/themen/2017/05/mit-daten-werte-schaffen---studie-2017.html, zuletzt abgerufen am 13.06.2017.
[3] Vgl. hierzu OLG Düsseldorf, Urt. v. 27.09.2012 – 6 U 241/11 – NJW-Spezial 2012, 759, welches das Bestehen eines Aussonderungsrechtes eines Insolvenzgläubigers an Kundendaten bejahte.
[4] LG Düsseldorf, Urt. v. 09.03.2016 – 12 O 151/15 – ZD 2016, 231, 233 unter Rn. 62.
[5] Ehmann, in: Simitis, BDSG, 8. Aufl. 2014, § 29 Rn. 2.
[6] In Anlehnung an Wandtke, MMR 2017, 6, 8.

2 Ausgangsfälle

Problemaufriss

Anwendungsfall 1

Das Unternehmen G vertreibt Gartenteiche. Über die Website des Unternehmens G ist es möglich, die Gartenteiche auch online zu bestellen. Hierbei muss der Kunde seine persönlichen Daten, wie beispielsweise Name und Adresse, in eine Maske eintragen und den entsprechenden Teich auswählen, damit der Vertrag erfolgreich abgewickelt werden kann. Die Konfiguration der Gartenteiche erfolgt mittels direkter Kommunikation zwischen Unternehmen und Kunde.

Anwendungsfall 2

Das Unternehmen G möchte nun ein Kundenportal mit einem sog. Gartenteich-Konfigurator einsetzen. Mithilfe des Gartenteich-Konfigurators kann der Kunde bestimmte Daten seines Grundstücks, wie beispielsweise Angaben über Größe, Form und Hangneigung, eingeben. Außerdem soll der Kunde persönliche Angaben machen, beispielsweise über sein Alter und die Anzahl der im Haushalt lebenden Personen. Hier ist insbesondere anzugeben, ob sich darunter Kinder befinden und wie alt diese sind. Auch Angaben zu einer etwaigen Bepflanzung oder Tierhaltung werden gefordert, ebenso wie über das Vorhandensein von Haustieren. Aufgrund dieser eingegebenen Daten wird dem Kunden daraufhin der Gartenteich, der am besten zu ihm und seinem Grundstück passt, angeboten.

Der Unternehmer G möchte die eingegebenen Daten seiner Kunden jedoch auch für andere Zwecke nutzen, beispielsweise, um seine Produkte zu verbessern, die Produktpalette an die von den Kunden am meisten nachgefragten Gartenteiche auszurichten und dem Kunden zusätzliche Artikel, beispielsweise Sicherungen zum Schutz kleiner Kinder, anzubieten. Anhand der Bepflanzung und Tierhaltung sollen die Intervalle für die Reinigung und Wartung des Gartenteichs bestimmt werden. Das Unternehmen G ist bereit, dem Kunden für die Angabe seiner Daten einen Preisnachlass für den Gartenteich zu gewähren.

Im Anwendungsfall 1 werden die Daten lediglich zur Vertragserfüllung benötigt, sie bilden dagegen nicht selbst den Gegenstand des Vertrags. Die Erhebung der persönlichen Daten des Kunden und die anschließende Nutzung für eigene Geschäftszwecke ist hierbei ohne Weiteres zulässig, da diese für die Begründung und Durchführung eines rechtsgeschäftlichen Schuldverhältnisses mit dem Betroffenen erforderlich sind

(§ 28 Abs. 1 Satz 1 Nr. 1 BDSG bzw. Art. 6 Abs. 1 Satz 1 lit. b DS-GVO). Würde der Unternehmer G nicht über die Daten seines Kunden verfügen, wüsste er beispielsweise nicht, an wen der Gartenteich geliefert werden sollte und die Durchführung des Vertrags wäre unmöglich. Daher ist eine Erhebung und Nutzung dieser Daten, die allein der Vertragserfüllung dienen, datenschutzrechtlich zulässig. Allerdings ist der Zweck der Erhebung und Nutzung der Daten bereits im Vorhinein konkret festzulegen (§ 28 Abs. 1 Satz 2 BDSG). Eine nachträgliche Zweckänderung ist im Falle der Verwendung der vorgenannten Daten zur Vertragserfüllung nicht möglich.

Im – in der Sache nur wenig abgewandelten und ergänzten – Anwendungsfall 2 erlangen die Daten dagegen einen Gegenleistungscharakter, da dem Kunden im Gegenzug zur Preisgabe seiner Daten ein Preisnachlass gewährt werden soll. Die Bereitstellung der Daten bildet somit bereits eine der Hauptleistungen des Vertrags. Aufgrund des Grundsatzes der Vertragsfreiheit ist die Festlegung von Daten als Gegenleistung durchaus möglich. Diese vertragliche Regelung gewährt dem Unternehmen G ein Zugriffsrecht auf die Daten des Betroffenen, welches jedoch aufgrund gesetzlicher oder gleichsam vertraglicher Vorgaben eingeschränkt sein kann.

Zunächst stellt sich – beiden Vertragspartnern – jedoch die Frage nach dem Wert der Daten, dessen Bestimmung große Schwierigkeiten bereitet. Dies ist unter anderem dem Umstand geschuldet, dass die Daten oft erst durch die nachträgliche Verknüpfung mit anderen Daten an Wert gewinnen. Eine erste Herausforderung wird daher sein, den Preisnachlass anhand der zur Verfügung gestellten Daten zu bestimmen. Überdies müssen zur Wirksamkeit des Vertrags die wesentlichen Vertragsinhalte genau festgeschrieben werden. Dies bedeutet in Bezug auf Daten, dass genau festgelegt werden muss, welche Daten für die Gewährung des Preisnachlasses zur Verfügung gestellt werden.

Wie bereits erwähnt, müssen bei der Verwendung von Daten als Gegenleistung auch bestimmte Grenzen beachtet werden. So darf die Erhebung und Verarbeitung der Daten nicht strafbar sein. Auch ist es Pflicht des Unternehmens G, die IT-Sicherheit zu gewährleisten. Dies bedeutet, dass die teilweise sehr sensiblen Daten vor unberechtigten Zugriffen von außen geschützt werden müssen. Sind personenbezogene Daten Vertragsgegenstand, so müssen auch die Anforderungen des Datenschutzrechts eingehalten werden. Das Datenschutzrecht steht in seiner Grundkonzeption einem Einsatz von Daten als Gegenleistung eher entgegen, sodass derzeit hohe datenschutzrechtliche Hürden bestehen.

Die Rechtsgrundlage des § 28 Abs. 1 Satz 1 Nr. 1 BDSG bzw. Art. 6 Abs. 1 Satz 1 lit. b DS-GVO ist – anders als im Anwendungsfall 1 – vorliegend nicht mehr erfüllt, sodass nach dem Grundsatz des Verbots mit Erlaubnisvorbehalt (§ 4 Abs. 1 BDSG bzw. Art. 6 Abs. 1 DS-GVO) die Einwilligung des Betroffenen in die Verarbeitung seiner Daten eingeholt werden muss. Diese ist neben der bloßen Hingabe der Daten – und neben dem (restlichen) Kaufpreis – als Hauptleistung geschuldet, da eine Verarbeitung der Daten nur bei Erteilung der datenschutzrechtlichen Einwilligung möglich ist. Die Einwilligung muss informiert erfolgen, was bedeutet, dass der Betroffene genau über die Art der

preisgegebenen Daten und deren beabsichtigte Verarbeitungszwecke aufgeklärt werden muss. Der Verarbeitungszweck ist daher bereits vorab zwingend festzulegen, weshalb das Unternehmen G von Anfang an wissen muss, für welche Zwecke die Daten verarbeitet werden sollen. Es ist von besonderer Wichtigkeit, gerade die datenschutzrechtlichen Anforderungen einzuhalten, da die ab dem 25. Mai 2018 geltende Datenschutz-Grundverordnung (DS-GVO) für Verstöße empfindliche Sanktionen vorsieht. Für die Verarbeitung personenbezogener Daten ohne Einwilligung des Betroffenen setzt die Datenschutz-Grundverordnung, sofern die Verarbeitung nicht durch eine gesetzliche Grundlage gedeckt ist, Bußgelder bis zu 20.000.000 EUR oder vier Prozent des gesamten weltweit erzielten Jahresumsatzes eines Unternehmens fest.

In diesem Zusammenhang ist zudem zu bedenken, dass sich eine Rückabwicklung des Vertrags, beispielsweise wenn der Gartenteich im genannten Fallbeispiel einen Mangel aufweist, gerade bei Daten als Gegenleistung sehr schwierig gestaltet, da die Daten bereits mit anderen Daten verknüpft sein könnten. Aus technischer Sicht empfiehlt es sich daher, dass der Datensatz stets im Ganzen löschbar bleibt. Insgesamt gilt, bereits im Vorhinein all diese Fragestellungen zu bedenken, um nachträgliche Schwierigkeiten vermeiden zu können.

Jedoch genügt es nicht, die einzelnen Rechtsgebiete isoliert zu betrachten. Vielmehr stehen alle Rechtsgebiete in einem engen Zusammenhang, sodass sich Verstöße auch auf andere Rechtsgebiete auswirken können. Es bestehen diverse Querbeziehungen zwischen den einzelnen Rechtsgebieten. Manche Verstöße – wie etwa eklatante Datenschutzverstöße – können beispielsweise die Nichtigkeit des abgeschlossenen Rechtsgeschäfts zur Folge haben, andere zu Ansprüchen auf Unterlassung oder auf Schadensersatz gegen das betreffende Unternehmen führen. Um die Risiken für das Unternehmen zu vermeiden, bedarf es mithin stets einer rechtsgebietsübergreifenden Betrachtung. Nur so kann eine rechtssichere Gestaltung für das Unternehmen gewährleistet werden.

3 Was versteht man unter Daten?

Definition und Eingrenzung

3.1 Unterschiedliches Begriffsverständnis

Der Begriff der „Daten“ ist in verschiedenen Rechtsgebieten von Relevanz – zu nennen ist natürlich das Datenschutzrecht, aber auch beispielsweise das Strafrecht. Auch deshalb hat sich noch kein einheitlicher Rechtsbegriff des „Datums“ bzw. von „Daten“ herausgebildet. Aufgrund des Vorschlags einer Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte[7] könnte auch im Zivilrecht der Begriff der „Daten“ eine noch größere Bedeutung erlangen.

Unter Daten im kommunikationswissenschaftlichen und auch im technischen Sinne sind die auf einem Datenträger festgehaltenen Zeichen oder Zeichenfolgen zu verstehen. Zeichen sind dabei zunächst interpretationsfreie Elemente der Sprache oder der Schrift, also etwa ein Symbol, eine Zahl oder ein Buchstabe, die sich mit ihrer Fixierung auf einem materiellen Datenträger von gesprochener Sprache und visueller Beobachtung unterscheiden.[8] Dies umfasst die syntaktische, vom Inhalt der Daten losgelöste Ebene.[9]

Beispiele

Daten, die in digitaler Form hergestellt oder bereitgestellt werden, sind beispielsweise Computerprogramme, Apps, Spiele, Musik, Videos oder Texte.[10]

Begibt man sich hingegen auf die semantische Ebene, misst man den Daten also eine Bedeutung bei, so handelt es sich streng genommen nicht mehr um Daten, sondern um Informationen.[11] Auf dieser Ebene differenziert beispielsweise das Datenschutzrecht über den Begriff der „personenbezogenen Daten“. Nur wenn personenbezogene Daten vorliegen, ist das Datenschutzrecht anwendbar und entfaltet seine Schutzwirkung für den Persönlichkeitsschutz. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 3 Abs. 1 BDSG). Auch in der DS-GVO ist der Begriff der personen-

[7] COM(2015) 634 final.
[8] Sieber, NJW 1989, 2569, 2572; Willke, Systemisches Wissensmanagement S. 7; Vesting in: Hoffmann-Riem/Schmidt-Assmann/Voßkuhle, Grundlagen des Verwaltungsrechts, Bd. II, 2. Aufl. 2012, § 20 Rn. 14; Albers in: Hoffmann-Riem/Schmidt-Assmann/Voßkuhle, Grundlagen des Verwaltungsrechts, Bd. II, 2. Aufl. 2012, § 22 Rn. 11.
[9] Stöhr, ZIP 2016, 1468; Zech, GRUR 2015, 1151, 1153.
[10] Siehe Erwägungsgrund 19 der Verbraucherrechte-Richtlinie, Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates vom 25. Oktober 2011.
[11] Stöhr, ZIP 2016, 1468; Zech, GRUR 2015, 1151, 1153.

bezogenen Daten definiert. Hiernach sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden: „betroffene 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 (Art. 4 Nr. 1 DS-GVO). Dabei ist es nicht zwingend notwendig, dass die Informationen, die zur Identifizierung einer Person erforderlich sind, nur einer einzigen Person zu Verfügung stehen müssen.[12] In Erwägungsgrund 26 der Richtlinie 95/46/EG heißt es: *„Bei der Entscheidung, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen."*

Ein Personenbezug ist daher bereits dann herstellbar, wenn die datenverarbeitende Stelle über rechtliche Mittel, beispielsweise über gesetzlich geregelte Auskunftsansprüche gegen Dritte, verfügt, die es ihr erlauben, den Betroffenen anhand der dadurch erhaltenen Informationen zu identifizieren.[13]

Beispiele

Personenbezogene Daten sind etwa Name, Alter, Herkunft, Geschlecht, Ausbildung, Familienstand, Geburtsdatum, aber auch das Vermögen, die Kreditwürdigkeit oder das Konsum- und Kommunikationsverhalten sowie die IP-Adresse.[14] Vor allem die IP-Adresse könnte bei sog. Smart Devices von erheblicher Bedeutung sein. Unter Smart Devices sind jederzeit nutzbare mobile Endgeräte zu verstehen, wie beispielsweise Smartphones, Tablets, Datenbrillen oder Smart Watches.[15] Neben genetischen Daten (Art. 4 Nr. 13 DS-GVO) und Gesundheitsdaten (Art. 4 Nr. 15 DS-GVO) werden auch biometrische Daten wie Gesichtsbilder oder Fingerabdrücke in der Datenschutz-Grundverordnung ausdrücklich als personenbezogene Daten eingestuft (Art. 4 Nr. 14 DS-GVO).[16]

Im Strafgesetzbuch (StGB) taucht der Begriff der Daten insbesondere bei den Straftatbeständen der §§ 202a ff. StGB und der §§ 303a ff. StGB auf. In diesem strafrechtli-

[12] EuGH, Urt. v. 19.10.2016 - C-582/14 - Breyer / Deutschland Tz. 43.
[13] EuGH, Urt. v. 19.10.2016 - C-582/14 - Breyer / Deutschland Tz. 49.
[14] Ernst, in: Paal/Pauly, Datenschutz-Grundverordnung, 2017, Art. 4 Rn. 14.
[15] Vgl. Kremer, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2. Aufl. 2016, § 28 Rn. 3.
[16] Vgl. hierzu ausführlich Ernst, in: Paal/Pauly, Datenschutz-Grundverordnung, 2017, Art. 4 Rn. 96 ff.

chen Kontext werden jedoch nur solche Daten erfasst, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden (§ 202a Abs. 2 StGB).

Beispiele

Erfasst werden Daten auf Festplatten, USB-Sticks oder Speicherkarten.[17] Nicht erfasst sind dagegen z. B. Barcodes auf Waren, nachdem deren Bedeutung unmittelbar visuell wahrnehmbar ist und diese lediglich entschlüsselt werden müssen, oder auch rein manuell erstellte Datensammlungen.[18] Ebenfalls nicht unter den genannten strafrechtlichen Datenbegriff fallen noch zu speichernde Inputdaten sowie bereits ausgedruckte Outputdaten.[19]

Demgegenüber hat der Begriff der Daten bislang noch keinen Eingang in das BGB gefunden. Das ist insofern bemerkenswert, als die unstreitige Bedeutung als Wirtschaftsgut eine Einordnung in das Zivilrecht nahelegt. In diese Richtung geht auch die derzeit heftig geführte Diskussion um ein „Dateneigentum“ – also etwa die Fragen, wem die Daten gehören bzw. wem sie zuzuordnen sind.

3.2 Einordnung in Fallgruppen

Wie Daten in (zivil-)rechtlicher Hinsicht eine Rolle spielen können, lässt sich mittels Fallgruppen veranschaulichen. Hierbei lassen sich im Wesentlichen fünf Kategorien ausmachen:

– Daten als Vertragserfüllungsvoraussetzung

In dieser Kategorie bilden die Daten nicht selbst den Gegenstand des Vertrags, sondern sie dienen lediglich der Vertragserfüllung. Die Daten sind also ein „bloßes Beiwerk“ des eigentlichen Vertrags, wie in Anwendungsfall 1 (oben, Kapitel 2).

Beispiel

Kauft man eine bestimmte Ware in einem Online-Shop, so werden für die Abwicklung des Kaufs der Name und die Anschrift des Käufers, die Art und die Menge des gekauften Artikels, die Zahlungsweise, die Versandangaben und gegebenenfalls auch die Kontoverbindung benötigt, um den Vertrag erfüllen zu können.[20]

---

[17] Graf, in: MüKo-StGB, 2. Aufl. 2012, § 202a Rn. 15.
[18] Lenckner/Eisele, in: Schönke/Schröder, StGB, 29. Aufl. 2014, § 202a Rn. 5 m.w.N.
[19] Lenckner/Eisele, in: Schönke/Schröder, StGB, 29. Aufl. 2014, § 202a Rn. 6.
[20] Taeger, in: Taeger/Gabel, BDSG, 2. Aufl. 2013, § 28 Rn. 52.

– Daten als Gegenleistung

Bei der Verwendung von Daten als Gegenleistung werden diese dagegen zum wesentlichen Vertragsinhalt. Nun stellen die Daten selbst eine Hauptleistungspflicht des schuldrechtlichen Verhältnisses dar. Ob und wie sich dies zivilrechtlich darstellen lässt, ist derzeit noch sehr umstritten.

Beispiel

Bei einer App, die vom Anbieter im App-Store kostenfrei zur Verfügung gestellt wird, bilden die Daten des Kunden die Gegenleistung zu ihrer Nutzung. Selbiges gilt etwa bei der – vermeintlich unentgeltlichen – Nutzung von sozialen Netzwerken oder Suchmaschinen. Weitere Beispiele sind der Erwerb von E-Books oder von Audioinhalten gegen bloße Zurverfügungstellung personenbezogener Daten. Kfz-Versicherungen bieten mittlerweile Telematik-Tarife an, die günstiger sind, wenn neben dem zu zahlenden Entgelt des Versicherers zugleich personenbezogene (Nutzungs-) Daten des PKW hingegeben werden, um eine bessere Risikoeinschätzung vornehmen zu können.

Die Ansicht, wonach die Daten hier Hauptleistungspflicht sind, scheint sich mittlerweile im zivilrechtlichen Schrifttum durchzusetzen, ohne dass hierzu (soweit ersichtlich) aber bereits Rechtsprechung existiert. In der Vergangenheit wurde mehrheitlich die Meinung vertreten, sofern Inhalte oder Leistungen unentgeltlich zur Verfügung gestellt würden, der Nutzer hierfür aber seine personenbezogenen Daten hingeben und die Einwilligung in die Verarbeitung dieser Daten erklären müsse, sei dies nicht die Gegenleistung aus dem Vertrag, sondern eine bloße Nebenleistungspflicht.[21]

Auch bei dem kommerziellen Handel mit Daten bilden diese letztlich die Gegenleistung des die Daten verkaufenden Unternehmens.[22]

– Daten als Gegenstand von Dienstleistungen

Ferner können Daten auch den Gegenstand bzw. das Ergebnis zahlreicher Anwendungen und Dienstleistungen bilden, ohne zugleich zur Vertragserfüllung zwingend notwendig zu sein oder die Gegenleistung als solches zu bilden. Zu nennen sind in diesem Zusammenhang insbesondere Big Data-Analysen und das Cloud Computing.

---

[21] Vgl. hierzu eingehend: Bräutigam, MMR 2012, 635, 635 ff.
[22] Vgl. hierzu eingehend: Specht, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung - Die zivilrechtliche Erfassung des Datenhandels, 2012.

– Datenverarbeitung als Vertragsgegenstand, z. B. Big Data-Analysen

Mithilfe von Big Data-Analysen sollen Datenmengen analysiert und eventuell sogar miteinander kombiniert werden, die zu groß und zu komplex sind und sich zu schnell ändern, als dass sie mit herkömmlichen Datenverarbeitungsmethoden ausgewertet werden könnten.[23]

Beispiele

Durch die Analyse von Prozessdaten in automatisierten Fertigungsprozessen kann eine schnelle Verarbeitung der Informationen in Echtzeit gewährleistet werden, um so den Fertigungsprozess optimal gestalten zu können.[24] Daten, die im Rahmen von Big Data-Analysen verwendet bzw. erst hieraus generiert werden, können aus zahlreichen unterschiedlichen Quellen stammen. So fallen etwa im Rahmen des vernetzten Kraftfahrzeugs („Smart Car") besonders viele Daten an, welche – wie bei sämtlichen vernetzten Technologien wie beispielsweise auch „Smart Home" oder „Smart Meter" – die Grundlage von Big Data-Analysen bilden können. Eine zusätzliche Besonderheit bei Big Data-Analysen besteht darin, dass die Zwecke, für die die Ergebnisse relevant werden, unter Umständen im Vornherein noch gar nicht bekannt sind, sondern sich erst durch die Analyse als solche ergeben.

– Datenspeicherung als Vertragsgegenstand, z. B. Cloud Computing

Beim Cloud Computing wird Rechnerleistung über das Internet zur Verfügung gestellt. Die Daten werden nicht auf einem lokalen Rechner, sondern in einer sog. „Datenwolke" gespeichert.[25] Dies bietet für die Anwender vor allem zwei Vorteile: Einerseits können sie so von überall aus auf ihre Daten zugreifen, andererseits bedarf es keiner kostenintensiven Vorhaltung lokaler Speicherplatzkapazitäten. Neben den Herausforderungen für die Datensicherheit geht es hier auch um Fragen des Datenschutzes. So werden in der Cloud zum Teil auch personenbezogene Daten gespeichert, auf die der Betreiber – je nach Ausgestaltung des Cloud-Dienstes, etwa in Bezug auf die Verschlüsselung der Daten – zumindest faktischen Zugriff hat.

---

[23] Vgl. Heckmann in: vbw-Studie: Big Data im Freistaat Bayern - Chancen und Herausforderungen, 2016, Teil II S. 87.
[24] Vgl. ausführlich zu diesem Fallbeispiel Heckmann in: vbw-Studie: Big Data im Freistaat Bayern - Chancen und Herausforderungen, 2016, Teil II S. 103.
[25] Weller/Nordmeier, in: Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, Rom II Art. 4 Rn. 15.

4 Wer darf auf die Daten zugreifen?

Interessen und Rechte der Beteiligten

In allen fünf Fallgruppen stellt sich die Frage, wer auf die anfallenden bzw. erzeugten Daten zugreifen darf. Um ihr zielgerichtet nachgehen zu können, muss zum einen festgestellt werden, welche Daten überhaupt erhoben wurden. Zum anderen bedarf es der Ermittlung der beteiligten Akteure, bei denen die Frage des rechtmäßigen Datenzugriffs überhaupt virulent werden kann, und ihrer jeweiligen Interessen.

Während im Beispiel des „Gartenteich-Konfigurators“ noch denkbar ist, dass außer dem Käufer nur noch das verkaufende Unternehmen beteiligt ist, welches – mit Blick auf den hausinternen Wartungs- und Reinigungsservice – ein Interesse am Zustand des Gartenteichs, der Art und Dauer der Ingebrauchnahme sowie generell den Nutzungsgewohnheiten des Käufers hat, kann demgegenüber die Vielfalt an verschiedenen Daten und die Anzahl der Interessenten hieran gerade im Kontext des Internet der Dinge („Internet of Things“, IoT) um ein Vielfaches höher ausfallen. Das IoT beschreibt die vollständige Vernetzung aller Lebensbereiche, durch die eine ständige Kommunikation zwischen einzelnen Geräten und die Auswertung der dadurch gesammelten Daten in Echtzeit gewährleistet werden können.

Einen Teilbereich hieraus bildet die Telematik. Dieser Begriff setzt sich aus den Begriffen „Telekommunikation“ und „Informatik“ zusammen und umfasst die Verknüpfung von Informationen mehrerer Systeme durch ein Telekommunikationssystem einschließlich einer besonderen Datenverarbeitung.[26] Einen besonderen Einsatzbereich findet die Telematik im Automobilsektor. Gerade moderne, vernetzte Kraftfahrzeuge produzieren erhebliche Datenmengen, die beispielsweise für den Halter des Fahrzeugs selbst oder den Hersteller, aber auch für IT-Unternehmen und Versicherer interessant sein können. Die Einsatzbereiche dieser Daten sind besonders vielfältig. Mithin eignet sich das Anwendungsbeispiel „Smart Car“ in besonderem Maße für die hier gegenständliche Thematik der Daten als Wirtschaftsgut.

4.1 Konkretes Anwendungsbeispiel: Daten im vernetzten Kraftfahrzeug („Smart Car“)

Ausgehend von der Feststellung, welche Daten überhaupt erhoben werden, soll im Rahmen des Anwendungsbeispiels „Smart Car“ der Frage nachgegangen werden, welche Interessen die beteiligten Akteure verfolgen.

[26] Kraus, DSRI-Tagungsband 2014, S. 377 f.

4.1.1 Erhobene Daten

Kraftfahrzeuge werden bereits jetzt als „rollende Computer“[27] bezeichnet. Daher überrascht es nicht, dass bei dem Betrieb eines Kraftfahrzeugs unzählige verschiedene und teils auch persönliche Daten preisgegeben werden. Teilweise verfügen moderne Fahrzeuge bereits über 80 Steuergeräte, die mithilfe von Sensoren die relevanten Daten ermitteln.[28] Schätzungen zufolge sind dies 25 Gigabyte pro Stunde und pro Fahrzeug.[29]

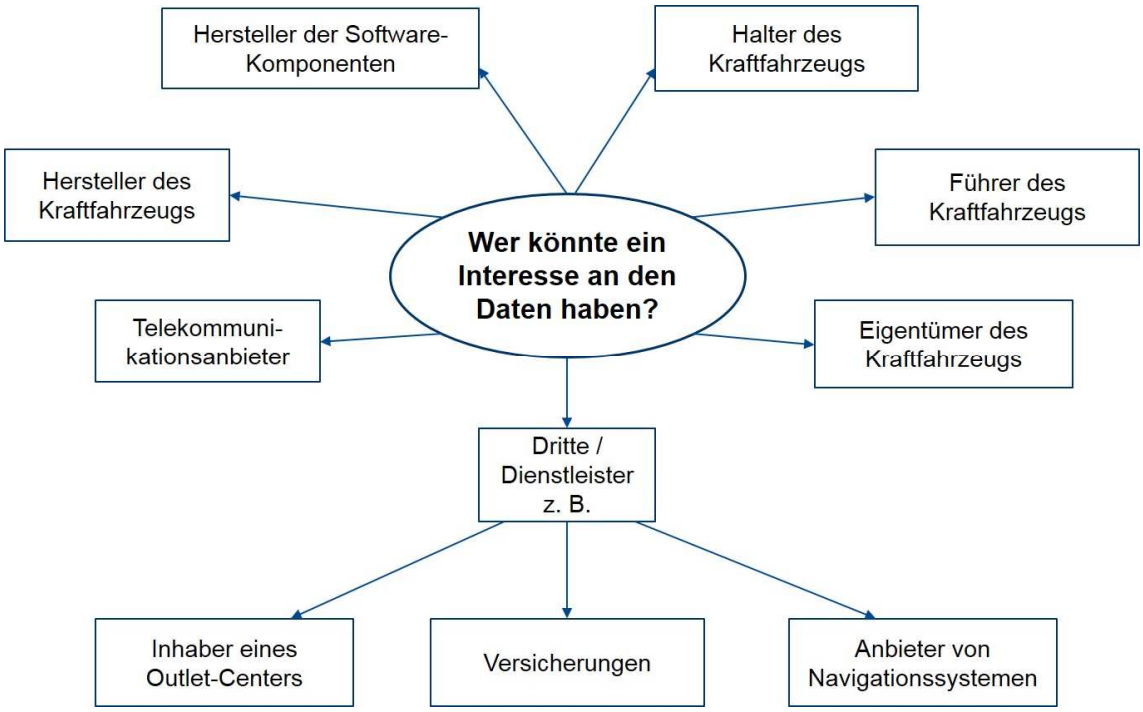
Für deren Erhebung im vernetzten Kraftfahrzeug kommen unter anderem folgende Daten in Betracht:[30]

- Angaben über das Fahrzeugumfeld, wie beispielsweise Daten über die Lichtverhältnisse, das Wetter oder Abstandsmessungen
- Daten über den Zustand des Kraftfahrzeugs, wie etwa über den Verbrauch des Autos, die Motortemperatur, den Reifendruck oder sonstige Verschleißerscheinungen
- Angaben über das Bewegungsprofil des Kraftfahrzeugs, so beispielsweise über die letzten angefahrenen Orte oder Reiseziele, die Fahrtdauer und die Fahrtstrecken
- Ermittlung von Daten der Beifahrer, beispielsweise wie viele Insassen wo in dem Fahrzeug saßen und ob diese alle angeschnallt waren
- Angaben über eine mögliche Ablenkung des Kraftfahrzeugführers, so etwa die Lautstärke der Musik im Inneren des Kraftfahrzeugs
- Daten über den Fahrstil (riskant oder eher gemächlich)
- Informationen über sonstige Fahrgewohnheiten des Kraftfahrzeugführers, wie beispielsweise Beschleunigungs- und Bremsverhalten, Motordrehzahl und Lenkverhalten
- Ermittlung fahrkritischer Gesundheitsdaten wie etwa der Pulsfrequenz, der Körperhaltung, der Feuchtigkeit der Hände, der Pupillenweite oder des Atemalkoholgehalts

[27] Lüdemann, ZD 2015, 247; v. Schönfeld, DAR 2015, 617, 618.
[28] Lüdemann, ZD 2015, 247.
[29] Vgl. Der Datenschutz kommt unter die Räder – Moderne Autos sammeln Gigabyte von Daten, abrufbar unter: http://www.3sat.de/page/?source=/nano/technik/192306/index.html, zuletzt abgerufen am 12.06.2017.
[30] Vgl. hierzu Lüdemann, ZD 2015, 247, 247 f.; v. Schönfeld, DAR 2015, 617, 618; Automatisiertes Fahren: Datenschutz und Datensicherheit, vbw 2018

4.1.2 Interessenlage der beteiligten Akteure

Abbildung 1
Darstellung möglicher Beteiligter und deren Interessen



Quelle: Eigene Darstellung

Die Interessenlage in diesem Mehrpersonenverhältnis ist vielschichtig und kompliziert: Dem Hersteller des Kraftfahrzeugs können diese gesammelten Daten bei der Verbesserung der Produktqualität von Nutzen sein. Gleiches gilt für die Hersteller der Softwarekomponenten des vernetzten Kraftfahrzeugs. Versicherungen könnten die Daten nutzen, um dem Halter speziell auf sein Fahrverhalten angepasste Versicherungstarife anzubieten („Pay as you drive“) oder auch Informationen über die Sicherheit des Fahrzeugs zu erlangen.[31] Privatwirtschaftliche Unternehmen, wie beispielsweise Hersteller von Navigationssystemen, könnten die Daten verwenden, um bestimmte Dienstleistungen, wie auf die Urlaubsreise abgestimmtes Kartenmaterial, zur Verfügung zu stellen.[32] Die Interessen des Halters, Führers oder Eigentümers des Kraftfahrzeugs, die nicht zwangsläufig in einer Person zusammenfallen müssen, sind etwa, Erkenntnisse über die Fahrweise oder die Arten der gesammelten Daten im Allgemeinen zu erhalten sowie verschiedene Komfortaspekte (positiv) oder die Ausspähung und die unbefugte Datenweitergabe an Dritte zu unterbinden (negativ). Aus diesem Interessengemenge

[31] Lüdemann, ZD 2015, 247, 248 f.
[32] Kraus, DSRI-Tagungsband 2014, S. 377, 378.

ergibt sich die Frage, wer auf die im Smart Car erzeugten Daten zugreifen darf und ggf. auch, wer Dritte von der Nutzung ausschließen darf.

4.2 Zugriffsbefugnis aus Dateneigentum?

In der juristischen Literatur ist eine Diskussion darüber entstanden, ob es ein Eigentum an Daten gibt. Das Eigentum gewährt dem Eigentümer umfassende Verfügungs- und Abwehrrechte. So kann der Eigentümer – soweit nicht das Gesetz oder Rechte Dritter entgegenstehen – mit der Sache nach Belieben verfahren und andere von jeder Einwirkung ausschließen (§ 903 BGB). Wird das Eigentum verletzt, stehen dem Eigentümer Schadensersatzansprüche (§ 823 BGB) zu. Eine Beeinträchtigung des Eigentums hat Ansprüche auf Beseitigung und Unterlassung (§ 1004 BGB) zur Folge. Würde man das Bestehen eines Dateneigentums bejahen, so könnte die Zugriffsbefugnis auf die im Smart Car erzeugten Daten daher unmittelbar aus dem absoluten Eigentumsrecht abgeleitet werden. Neben der Frage, „ob“ es ein Dateneigentum gibt, stellt sich ggf. die Anschlussfrage, „wer“ dann der Eigentümer der jeweiligen Daten wäre (im Beispiel des vernetzten Fahrzeugs: Fahrer, Halter, Eigentümer, Hersteller etc.)

Der Ausgangspunkt dieser aktuellen Diskussion besteht darin, dass das BGB in seinen zivilrechtlichen Eigentumsvorschriften das Eigentum an Sachen nur auf körperliche Gegenstände bezieht (§ 903 Satz 1, § 90 BGB). Ein Datum als solches ist jedoch gerade kein körperlicher Gegenstand.[33]

Sind die Daten auf einem körperlichen Datenträger, wie beispielsweise einem USB-Stick (oder im konkreten Anwendungsfall nach Kapitel 4.1 stationär im Pkw), gespeichert, so vermittelt der körperliche Datenträger, der über die Eigentumsvorschriften geschützt ist, auch einen Schutz der Daten. Werden auf einem Datenträger gespeicherte Daten verändert, so führt dies automatisch auch zu einer Änderung der magnetischen Struktur des Datenträgers, sodass eine Eigentumsverletzung am Trägermedium vorliegt.[34] Das Datum genießt daher nur einen mittelbaren Schutz, der über den Datenträger vermittelt wird.[35] Keinesfalls aber bedeutet ein aus dem Träger-medium folgender Schutz gegen Verletzungen respektive Löschung der Daten, dass sie eigentumsrechtlich dem Eigentümer des Trägermediums zugeordnet sind. Allen Immaterialgütern liegt es zugrunde, dass die Zuordnung möglicher ausschließlichkeits-rechtlicher Befugnisse unabhängig vom Eigentum am Trägermedium erfolgt.

---

[33] Heckmann, in: vbw-Studie: Big Data im Freistaat Bayern - Chancen und Herausforderungen, 2016, Teil II S. 113.
[34] OLG Karlsruhe, Urt. v. 07.11.1995 – 3 U 15/95 – NJW 1996, 200; Wagner, in: MüKo-BGB, 7. Aufl. 2017, § 823 Rn. 220.
[35] Heckmann, in: vbw-Studie: Big Data im Freistaat Bayern - Chancen und Herausforderungen, 2016, Teil II S. 113.

Beispiel

Das Eigentum an einer CD bedeutet nicht, dass der Eigentümer auch Inhaber der Urheberrechte an dem auf der CD gespeicherten Musikwerk ist.
Eine Zuordnung ausschließlichkeitsrechtlicher Befugnisse an den Eigentümer des Trägermediums scheitert aber spätestens dort, wo Daten ohne Bezug zu einem Datenträger online übermittelt werden, was im Hinblick auf das Cloud Computing immer häufiger der Fall ist.[36] Grundgesetzliche und datenschutzrechtliche Wertungen würden grob missachtet, ließe man dem Eigentum am Cloud-Server automatisch das „Eigentum" an allen dort gespeicherten Daten der Nutzer folgen. Da in der heutigen Zeit die Speicherung auf lokalen Datenträgern immer mehr an Bedeutung verliert und die Daten stattdessen häufig in der Cloud gespeichert oder ohne Bezug zu einem Datenträger online übermittelt werden, scheidet die Anknüpfung an körperliche Datenträger außerdem zunehmend aus und der Schutz durch die Eigentumsvorschriften geht ins Leere.

Beispiel

Bei der Eingabe von Daten in ein Online-Formular, beispielsweise bei der Anmeldung in einem sozialen Netzwerk oder bei einem Einkauf über eine Online-Handelsplattform oder ein Online-Versteigerungsportal, findet die Übermittlung und Speicherung ohne einen körperlichen Datenträger statt.

Es existiert also nach derzeit geltendem Recht gerade kein Eigentumsrecht an Daten im Sinne des § 903 BGB.[37]

(Einzel-)Daten sind auch nicht Gegenstand des Urheberrechts, da das Urheberrecht eine sogenannte geistige Schöpfung erfordert. D.h. es ist ein gewisser Grad an geistiger Leistung, an schöpferischer Eigentümlichkeit erforderlich, um von einem urheberrechtlich schutzfähigen Werk zu sprechen. Das Urheberrecht kennt zwar auch einen nicht-schöpferischen Datenbankschutz gemäß §§ 87a ff. UrhG.

§ 87a Abs. 1 Satz 1 UrhG (Definition Datenbank)

Datenbank im Sinne dieses Gesetzes ist eine Sammlung von Werken, Daten oder anderen unabhängigen Elementen, die systematisch oder methodisch angeordnet und einzeln mit Hilfe elektronischer Mittel oder auf andere Weise zugänglich sind und deren Beschaffung, Überprüfung oder Darstellung eine nach Art oder Umfang wesentliche Investition erfordert.

[36] Sprau, in: Palandt, BGB, 75. Aufl. 2016, § 823 Rn. 9.
[37] Heckmann, in: vbw-Studie: Big Data im Freistaat Bayern - Chancen und Herausforderungen, 2016, Teil II S. 113.

Geschützt sind hier aber nur Datenbanken, d. h. gerade keine Einzeldaten, die ein mögliches Eigentumsrecht an Daten adressieren könnte.

Neben der Diskussion, ob ein Dateneigentum bereits aus den zivilrechtlichen Vorschriften folgt, existieren weitere Ansätze zur Etablierung eines Dateneigentums. So wird beispielsweise vertreten, über die Zuordnung von Ausschließlichkeitsrechten ein Dateneigentum als „eigentumsartiges Recht" zu etablieren.[38] Die Diskussion ist allerdings noch nicht abgeschlossen.[39]

Zur Beantwortung der Frage, ob es ein Eigentumsrecht an Daten selbst geben könnte bzw. sollte, werden in der rechtswissenschaftlichen Literatur verschiedene Ansätze vertreten.[40] Im Vordergrund steht vor allem der Gedanke, dass das Zivilrecht mit der digitalen Entwicklung Schritt halten und daher auch ein Eigentumsrecht an Daten gewährleisten müsse, um der Realität klare „Spielregeln" aufzuzeigen.[41] Die überwiegende Ansicht spricht sich unterdessen gegen ein Dateneigentum im Sinne der zivilrechtlichen Vorschriften des BGB aus.[42] Dies gilt sowohl für die Zuordnung von Daten unter den „Eigentumsbegriff" als auch für die Subsumtion unter ein „sonstiges Recht" i.S.d. § 823 Abs. 1 BGB.

Auch in der Politik gewinnt die Frage um das Bestehen eines Dateneigentums immer mehr an Bedeutung. Bundeskanzlerin Angela Merkel sprach sich anlässlich der CeBIT 2017 für das umstrittene Eigentumsrecht an Daten aus und bezog sich insbesondere auf die in den vernetzten Kraftfahrzeugen erzeugten personenbezogenen Daten. Sie stellte jedoch nur den Hersteller des Kraftfahrzeugs und den Hersteller der Software als mögliche Eigentümer der Daten zur Wahl, sodass nach ihrer Auffassung nur Unternehmen und mithin keine natürlichen Personen hierfür in Betracht kommen. Um diese Frage schnell und vor allem einheitlich zu klären, fordert Angela Merkel eine zügige und klare Rechtssetzung innerhalb der Europäischen Union.[43] Diese Bestrebung steht auch im Einklang mit der sog. „Strategie für einen digitalen Binnenmarkt für Europa" der Europäischen Kommission vom 06. Mai 2015[44] mitsamt dem zugehörigen Maßnahmenpaket („Industry Package"), das seinerseits am 19. April 2016 veröffentlicht

[38] Vgl. hierzu Zech, GRUR 2015, 1151.
[39] Vgl. hierzu Kraus, DSRI-Tagungsband 2014, S. 377, 379 f., Arkenau/Wübbelmann, DSRI-Tagungsband 2015, S. 95, 108.
[40] Vgl. hierzu Kraus, DSRI-Tagungsband 2014, S. 377 ff., Arkenau/Wübbelmann, DSRI-Tagungsband 2015, S. 95 ff.
[41] Vgl. hierzu beispielsweise Wagner, in: MüKo-BGB, 7. Aufl. 2017, § 823 Rn. 294.
[42] So etwa Roßnagel, NJW 2017, 10, 11; grundsätzlich ablehnend Hornung/Hofmann, Rechtsfragen bei Industrie 4.0: Rahmenbedingungen, Herausforderungen und Lösungsansätze, in: Reinhart, Handbuch Industrie 4.0, 2017, S. 191, 198.
[43] Dachwitz, Dateneigentum: Merkel ist noch unsicher, ob unsere Daten Firma A oder Firma B gehören sollen, abrufbar unter: https://netzpolitik.org/2017/dateneigentum-merkel-ist-noch-unsicher-ob-unsere-daten-firma-a-oder-firma-b-gehoeren-sollen/, zuletzt abgerufen am 02.06.2017.
[44] COM(2015) 192 final.

wurde.[45] Die Europäische Kommission schlägt ein data producer`s right vor, will hiervon allerdings allein nicht-personenbezogene Daten erfasst wissen.

Das Bundesministerium für Verkehr und digitale Infrastruktur plant demgegenüber, Daten im Ergebnis mit Sachen gleichzustellen, sodass diese eindeutig einem Eigentümer zugewiesen werden können und mithin – anders als nach dem Vorschlag der Bundeskanzlerin – auch z. B. der Halter des Kraftfahrzeugs als möglicher Dateneigentümer in Betracht kommt. Dies zeigt das Mitte 2016 veröffentlichte „Strategiepapier digitale Souveränität".[46] Die Notwendigkeit dieser Gleichstellung begründete der damalige Bundesminister mit den Herausforderungen, die aufgrund der zunehmenden Vernetzung der Automobilindustrie entstehen würden.[47] Dieser Vorschlag blieb jedoch abermals nicht ohne Kritik.[48]

Trotz dieser Bestrebungen in der Politik, ein Dateneigentum zu etablieren, bleibt die weitere Entwicklung dieser Diskussion ungewiss. Es spricht vieles dafür, dass es vorerst keine gesetzlichen Neuregelungen eines Dateneigentums (etwa durch Präzisierung oder Ergänzung des Eigentumsbegriffs i.S.d. §§ 823, 903 BGB)[49] geben wird, sondern die Handhabung des Datenumgangs und der Datenverwertung in der Praxis abgewartet und erprobt werden soll. Das ist begrüßenswert. Im Prinzip genügt das geltende Recht, die wesentlichen Interessenkonflikte zu lösen. So enthält auch das Datenschutzrecht, insbesondere die Datenschutzgrundverordnung, Regelungen zu Schutz und Zugriff auf Daten, etwa im Rahmen des Einwilligungsmanagements oder der Interessenabwägung.

4.3 Zugriffs- und Nutzungsbeschränkungen an Daten?

Nach geltender Rechtslage besteht ein Eigentumsrecht an Daten ebenso wenig wie eigentumsähnlich ausgestaltete Rechtspositionen. Dies hat zur Folge, dass grundsätzlich sämtliche Akteure, denen ein faktischer Datenzugriff möglich ist, die Daten auch nutzen dürfen, soweit nicht bestimmte Zugriffs- und Nutzungsbeschränkungen beste-

---

[45] Weiterführende Informationen abrufbar unter: https://ec.europa.eu/digital-single-market/en/digitising-european-industry, zuletzt abgerufen am 13.06.2017. Vgl. auch die übersichtliche Darstellung bei Becker, GRUR Newsletter 01/2016, S. 7, 10.
[46] https://www.bmvi.de/SharedDocs/DE/Artikel/K/dobrindt-strategie-fuer-digitale-souveraenitaet.html, zuletzt abgerufen am 11.06.2017.
[47] Dachwitz, Dateneigentum: Merkel ist noch unsicher, ob unsere Daten Firma A oder Firma B gehören sollen, v. 20.03.2017, abrufbar unter: https://netzpolitik.org/2017/dateneigentum-merkel-ist-noch-unsicher-ob-unsere-daten-firma-a-oder-firma-b-gehoeren-sollen/, zuletzt abgerufen am 02.06.2017.
[48] Krempl, Datenausweis fürs Auto: Dobrindts Initiative zum Dateneigentum erntet Kritik, abrufbar unter: https://www.heise.de/newsticker/meldung/Datenausweis-fuers-Auto-Dobrindts-Initiative-zum-Dateneigentum-erntet-Kritik-3666889.html, zuletzt abgerufen am 02.06.2017.
[49] Vgl. zu entsprechenden Vorschlägen auch die Studie des BMVI „Eigentumsordnung für Mobilitätsdaten", 2017, an der Wissenschaftler von Partnerschaft Deutschland, dem Lorenz-von-Stein-Institut für Verwaltungswissenschaften an der Christian-Albrechts-Universität zu Kiel, der Universität Kassel sowie dem Fraunhofer Institut FOKUS mitgewirkt haben.

hen, die sich insbesondere aus dem Straf-, Wettbewerbs- und Datenschutzrecht ergeben. Darüber hinaus können auch vertragliche Beschränkungen des Datenzugriffs bestehen.

4.3.1 Straf- und Wettbewerbsrecht

In straf- und wettbewerbsrechtlicher Hinsicht können vor allem folgende Vorschriften relevant werden, die den Daten einen besonderen Rechtsgüterschutz zuweisen:

– §§ 303a ff. StGB

Der Straftatbestand der Datenveränderung nach § 303a StGB[50] schützt die Verfügungsgewalt des Berechtigten über die in Datenspeichern enthaltenen Informationen.[51] § 303a Abs. 1 StGB stellt somit das rechtswidrige Löschen, Unterdrücken, Unbrauchbarmachen und Verändern von Daten unter Strafe. Nach § 303a Abs. 3 StGB wird auch die Vorbereitung einer derartigen Straftat unter Strafe gestellt.

Beispiel

Das Löschen von Daten setzt voraus, dass eine Rekonstruktion der Daten nicht mehr möglich ist. Daher fällt neben dem Löschen von Daten und E-Mails auch das Überschreiben von Daten oder der Einsatz von Viren, die zu einer irreversiblen Aufhebung des Datenzusammenhangs führen, unter den Tatbestand des § 303a Abs. 1 StGB.[52]

Die nach § 303b StGB strafbare Computersabotage bezweckt den Schutz des Interesses am störungsfreien Funktionieren der Datenverarbeitung.[53] Geahndet wird daher die erhebliche Störung einer Datenverarbeitung, die für einen anderen von erheblicher Bedeutung ist (§ 303b Abs. 1 StGB).

Beispiel

Eine erhebliche Störung sind etwa technische Funktionsbeeinträchtigungen oder Programmveränderung, die den Absturz des gesamten Systems zur Folge haben.[54]

– §§ 202a ff. StGB

[50] Vgl. hierzu Kuhls, AnwZert ITR 11/2017 Anm. 3.
[51] Fischer, StGB, 63. Aufl. 2016, § 303a Rn. 2; BT-Drs. 10/5058, S. 34.
[52] Fischer, StGB, 63. Aufl. 2016, § 303a Rn. 9.
[53] BT-Drs. 10/5058, S. 35; zum Schutzzweck differenzierend Fischer, StGB, 63. Aufl. 2016, § 303b Rn. 2.
[54] Weidemann in: v. Heintschel-Heinegg, Beck-OK StGB, 34. Edition, Stand: 01.05.2017, § 303b Rn. 14.

Der Straftatbestand des Ausspähens von Daten gemäß § 202a Abs. 1 StGB stellt es unter Strafe, sich oder einem anderen durch die Überwindung von Sicherungsmaßnahmen unberechtigt Zugang zu Daten zu verschaffen, die nicht für ihn bestimmt und gegen unberechtigten Zugang besonders gesichert sind. Dies gilt auch für das unberechtigte Abfangen von nicht für den Täter bestimmten Daten aus einer nicht öffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage unter Verwendung technischer Mittel (§ 202b StGB).

Beispiel

Wird ein Computer durch technische Maßnahmen derart manipuliert, dass die Chatnachrichten des Benutzers aus einem nicht öffentlichen Chat auf den Computer einer anderen Person umgeleitet und aufgenommen werden, so ist der Straftatbestand des § 202b StGB erfüllt.[55]

Wer eine der beiden Taten vorbereitet (§ 202c StGB) oder Daten, die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, überlässt, verbreitet oder sonst mit Bereicherungsabsicht zugänglich macht (§ 202d StGB), muss ebenfalls mit Strafen rechnen.

– §§ 17 ff. UWG

Gemäß § 17 Abs. 1 UWG wird bestraft, wer als Mitarbeiter eines Unternehmens ein ihm im Rahmen des Dienstverhältnisses anvertrautes oder zugänglich gewordenes Geschäfts- oder Betriebsgeheimnis während der Geltungsdauer des Dienstverhältnisses unbefugt einem Dritten mitteilt, um sich oder einen Dritten zu begünstigen oder um dem Unternehmen zu schaden. Gleiches gilt gem. § 18 Abs. 1 UWG für die unbefugte Verwertung oder Mitteilung von Vorlagen oder Vorschriften technischer Art zu Zwecken des Wettbewerbs oder aus Eigennutz. Neben dem Versuch dieser Straftaten ist auch bereits der Versuch des Anstiftens oder die Verabredung zu einer Tat nach § 17 oder § 18 UWG gemäß § 19 UWG strafbar.

Beispiel

Unter Betriebs- und Geschäftsgeheimnisse fallen etwa Computerprogramme, Kalkulationsunterlagen und einzelne Umstände konkreter Geschäftsbeziehungen zu bestimmten Kunden oder Kundenlisten und Kundendaten.[56]

[55] AG Kamen, Urt. v. 04.07.2008 – 16 Ds 104 Js 770/07 – 67/08.
[56] Vgl. Harte-Bavendamm in: Harte-Bavendamm/Henning-Bodewig, UWG, 4. Aufl. 2016, § 17 Rn. 7.

Während die strafrechtlichen Vorschriften aufgrund der doch hohen Anforderungen nur selten verwirklicht sein dürften, hat der Geheimnisschutz des Wettbewerbsrechts erhebliche praktische Bedeutung. Daten können durchaus Geschäftsgeheimnisse sein, die über §§ 17, 18 UWG geschützt sind. Der Begriff des Geschäfts- oder Betriebsgeheimnisses erfasst in ständiger Rechtsprechung jede im Zusammenhang mit einem Betrieb stehende Tatsache, die nicht offenkundig, sondern nur einem eng begrenzten Personenkreis bekannt ist und nach dem Willen des Betriebsinhabers aufgrund eines berechtigten wirtschaftlichen Interesses geheim gehalten werden soll.[57] Technisches Wissen wird dabei als Betriebsgeheimnis, kaufmännisches als Geschäftsgeheimnis bezeichnet.[58] Es besteht Schutz gegen die Verletzung von Geschäftsgeheimnissen aber nur, solange die betreffenden Daten faktisch geheim gehalten und nicht offenkundig werden.

4.3.2 Datenschutzrecht

Datenschutzrechtliche Vorgaben finden nur dann Anwendung, wenn Schutzgüter des Datenschutzrechts betroffen sind. Dabei handelt es sich um jegliche Informationen, die sich auf eine bestimmte bzw. identifizierte oder bestimmbare bzw. identifizierbare natürliche Person beziehen und damit unmittelbar oder mittelbar einen Personenbezug aufweisen (vgl. § 3 Abs. 1 BDSG bzw. Art. 4 Nr. 1 EU-DSGVO).

Beispiel

Personenbezogene Daten sind beispielsweise der Name, das Geburtsdatum, Kreditkartendaten, (E-Mail-)Adressen oder IP-Adressen. Dagegen fallen reine Statistiken ohne Personenbezug, Busfahrpläne oder Aktienkurse nicht unter den Begriff der personenbezogenen Daten.

Um den Regelungen des Datenschutzrechts nicht zu unterfallen, besteht jedoch auch die Möglichkeit, den Personenbezug durch Anonymisierung aufzulösen. § 3 Abs. 6 BDSG definiert den Begriff des Anonymisierens wie folgt:

Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

[57] BGH, Urt. v. 15.03.1955 - I ZR 111/53, GRUR 1955, 424 – Möbelpaste; BGH, Urt. v. 01.07.1960 – I ZR 72/59, GRUR 1961, 40, 43 – Wurftaubenpresse; BGH, Urt. v. 27.04.2006 – I ZR 126/03, GRUR 2006, 1044, 1046 – Kundendatenprogramm; die Voraussetzung des Geheimhaltungswillens ist dabei nach z.T. vertretener Ansicht entbehrlich, vgl.: Brammsen in: MüKo Lauterkeitsrecht, 2. Aufl. 2014, § 17 UWG Rn. 9; zum Ganzen: Harte-Bavendamm in: Harte-Bavendamm/Hennig-Bodewig, UWG, 4. Aufl. 2016, § 17 Rn. 1; Specht, CR 2016, 288, 288 ff.
[58] Harte-Bavendamm in: Harte-Bavendamm/Hennig-Bodewig, UWG, 4. Aufl. 2016, § 17 Rn. 1.

Dabei ist aber rechtlich umstritten, ob der Anonymisierungsprozess selbst erlaubnispflichtig im Sinne des Datenschutzrechts ist. Vorsorglich empfiehlt sich daher die Einholung einer Einwilligung des Betroffenen bei jedem Anonymisierungsvorgang. Daran ergibt sich auch unter der Datenschutz-Grundverordnung keine Änderungen. Die Verordnung enthält dabei bemerkenswerterweise keine eigene Definition des Anonymisierens, sondern erwähnt dies nur noch in den Erwägungsgründen (Nr. 26 Sätze 5 und 6 DS-GVO).

Soweit die datenschutzrechtlich relevanten Vorgänge dem Datenschutzrecht unterfallen, bedarf es nach dem sog. Verbot mit Erlaubnisvorbehalt, das in § 4 Abs. 1 BDSG bzw. Art. 6 Abs. 1 DS-GVO geregelt ist, entweder einer gesetzlichen Ermächtigung oder einer Einwilligung des Betroffenen:

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Erlaubnistatbestände sind auf viele verschiedene Gesetze verteilt und haben auch innerhalb dieser eine teils sehr komplexe und unübersichtliche Ausgestaltung erfahren (vgl. etwa §§ 28, 29, 32 BDSG, §§ 14, 15 TMG, §§ 95, 96 TKG).

Beispiele

Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist die Erhebung, Speicherung, Veränderung und Übermittlung der Daten und die Nutzung der Daten für eigene Geschäftszwecke zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist. Dies betrifft die Fallgruppe der Daten als Vertragserfüllungsvoraussetzung (vgl. hierzu unter 3.2.). Sehr ähnliche Vorgaben finden sich in Art. 6 Abs. 1 lit. b, c DS-GVO.

Eine entsprechende Regelung für Telemedien findet sich in § 14 Abs. 1 TMG, wonach personenbezogene Daten eines Nutzers nur erhoben und verwendet werden dürfen, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind. Dies umfasst beispielsweise die Registrierungsdaten bei einem sozialen Netzwerk wie Benutzername, Passwort und E-Mail-Adresse.[59]

Aufgrund der allgemeinen Geltung der Datenschutz-Grundverordnung als europäische Verordnung mit unmittelbarem Anwendungsvorrang gegenüber entgegenstehendem

[59] Spindler/Nink in: Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, § 14 TMG Rn. 3.

nationalen Recht (vgl. Art. 288 Abs. 3 AEUV) sind jedoch einige Erlaubnistatbestände seit dem 25. Mai 2018 teilweise vollständig nicht mehr anwendbar, darunter etwa die §§ 11 ff. TMG. Der bayme vbm-Leitfaden *Datenschutzrecht 2018* bietet speziell zu dieser Thematik eine gute Orientierungshilfe.

Aufgrund der teils sehr komplexen und unübersichtlichen Ausgestaltung empfiehlt es sich, in Zweifelsfällen stets eine Einwilligung des Betroffenen einzuholen. Hierbei sind jedoch wiederum einige Anforderungen zu berücksichtigen, wie etwa die Informiertheit der Einwilligung (siehe hierzu im Einzelnen unter 7.).

Beispiel

---

§ 4a Abs. 1 Satz 2 BDSG bzw. Art. 6 Abs. 1 lit. a DS-GVO fordern, dass der Betroffene auf den vorgesehenen Zweck der Datenverarbeitung hingewiesen wird. Gibt etwa ein Betreiber eines sozialen Netzwerks die Daten an einen Online-Spieleanbieter weiter, so genügt es nicht, wenn der einzelne Nutzer nur auf die Weitergabe als solche hingewiesen wird, es muss auch der Datenempfänger mitgeteilt werden.

4.3.3 Vertragliche Regelungen

Neben gesetzlichen Vorgaben besteht auch die Möglichkeit, den Zugriff auf die Daten mitsamt deren Verwendung vertraglich zu regeln. Dies ist Ausfluss der Privatautonomie im deutschen Zivilrecht und dient der Selbstregulierung des Datenzugriffs und nachfolgender Verwendung. Die Einräumung ausschließlicher Nutzungsrechte an personenbezogenen Daten wird jedoch mit Blick auf die in Art. 1 Abs. 1 GG gewährleistete Menschenwürde nicht möglich sein.[60] Das ausschließliche Nutzungsrecht ist (natürlich nur für urheberrechtliche Werke, nicht für nicht-urheberrechtsschutzfähige Daten) in § 31 Abs. 3 Satz 1 UrhG geregelt:

Das ausschließliche Nutzungsrecht berechtigt den Inhaber, das Werk unter Ausschluss aller anderen Personen auf die ihm erlaubte Art zu nutzen und Nutzungsrechte einzuräumen.

Bei der Einräumung eines derartigen ausschließlichen Nutzungsrechts könnte auch der Betroffene selbst von der Nutzung seiner eigenen persönlichen Daten ausgeschlossen werden. Da der Betroffene bei jeder wirtschaftlichen oder sozialen Interaktion seine persönlichen Daten benötigt, würde ihm jedwede derartige Interaktion – in Bezug auf die konkret in Rede stehenden personenbezogenen Daten – nicht mehr gestattet, was unter Umständen zu einer erheblichen Beeinträchtigung der Lebensstellung des Betroffenen führen würde. Hinzu kommt, dass die personenbezogenen Daten dann auch

---

[60] Specht, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung: Die zivilrechtliche Erfassung des Datenhandels, 2012, Kap. 6 Rn. 337.

nur dem Willen desjenigen, dem das ausschließliche Nutzungsrecht eingeräumt wurde, unterliegen würden. Ein derartig gänzlicher Ausschluss des Betroffenen ist – soweit es jedenfalls um mehr als nur vereinzelte, eher belanglose Daten geht – mit der Garantie der Menschenwürde nicht vereinbar.[61] In Betracht käme daher nur die Einräumung eines einfachen, gerade nicht ausschließlichen Nutzungsrechts. Dieses ist (wiederum nur beispielshafte Nennung, in Betracht kommt allenfalls eine Anwendung des Rechtsgedankens) in § 31 Abs. 2 UrhG näher geregelt:

Das einfache Nutzungsrecht berechtigt den Inhaber, das Werk auf die erlaubte Art zu nutzen, ohne dass eine Nutzung durch andere ausgeschlossen ist.

Des Weiteren sind auch hier sonstige Beschränkungen aus dem geltenden Recht zu beachten (siehe die Darstellung der Querbeziehungen unter 9.).

[61] Specht, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung: Die zivilrechtliche Erfassung des Datenhandels, 2012, Kap. 6 Rn. 331 f.

5 Welchen Wert haben Daten?

Eine Gretchenfrage der digitalen Transformation

Dass Daten, vor allem im digitalen Raum, einen ökonomischen Wert haben, ist unbestritten.[62] Nicht nur Sachdaten können einen enormen wirtschaftlichen Wert aufweisen.[63] Auch personenbezogene Daten sind oft Teil der Vermarktungsstrategie von Produkten und Dienstleistungen, auch werden sie als eigener Produktionsfaktor bezeichnet.[64] Sie nehmen damit eine wichtige Rolle im Warenzyklus ein.[65] Der ihnen hierdurch zukommende Wert macht sie zudem für den Datenhandel attraktiv. Den wirtschaftlichen Wert von Daten präzise zu bestimmen, stellt jedoch eine große Herausforderung dar.[66]

Die Werbebranche nutzte bereits vor der Digitalisierung personenbezogene Daten bestimmter Personen, beispielsweise Bildnisse Prominenter zu Merchandising-Zwecken.[67] Die Verwendung personenbezogener Daten potenzieller Kunden zu Geschäftszwecken gewann dagegen erst durch die Möglichkeit des Anlegens von Nutzerprofilen und der damit verbundenen individualisierten (Online-)Werbung an Bedeutung. Auch die Nutzung von Daten zur Entwicklung von Dienstleistungen und Produkten kam erst durch die fortschreitende Digitalisierung und die Möglichkeit der Auswertung großer Datenmengen auf. Der stetig wachsende wirtschaftliche Wert von Daten wird auch durch einen Blick auf den Big Data-Sektor deutlich, der einer Mitteilung der Europäischen Kommission von 2015 zufolge jährlich um 40 Prozent wächst[68] und bereits heute rund 0,3 Prozentpunkte zum jährlichen Wachstum der deutschen Bruttowertschöpfung beiträgt[69].

Durch die doppelte Nutzbarkeit der Daten für die Entwicklung und Vermarktung von Produkten und Dienstleistungen (*Gebrauchswert* von Daten) entstand auch ein von den Marktmechanismen Angebot und Nachfrage bestimmter Datenhandel. Hierbei wer-

---

[62] Langhanke/Schmidt-Kessel, EuCML 2015, 218, 219.
[63] Vgl. etwa zum wirtschaftlichen Wert von Open (Government) Data: Heckmann, in: vbw-Studie: Open Data – Rechtliche Bewertung, 2017, S. 2 ff. Vgl. ferner zu den ökonomischen Aspekten der Digitalisierung u.a. in Gestalt des Produktionsfaktors Informationen: Lichtblau et al., in: vbw-Studie: Neue Wertschöpfung durch Digitalisierung, 2017. Teil I Kap. A S. 52 ff.
[64] Wandtke, MMR 2017, 6, 7; Zech, GRUR 2015, 1151.
[65] Wandtke, MMR 2017, 6, 7.
[66] Vgl. eingehend etwa die vbw-Studie Neue Wertschöpfung durch Digitalisierung, 2017
[67] Vgl. Schulze in: Dreier/Schulze, UrhG, 5. Aufl. 2015, Vorbemerkung zu §§ 31 ff. Rn. 186.
[68] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Strategie für einen digitalen Binnenmarkt für Europa, 06.05.2015, COM(2015), 192 final, S. 16.
[69] Beinahe deckungsgleich für den Freistaat Bayern: Prognos AG, in: vbw-Studie: Big Data im Freistaat Bayern – Chancen und Herausforderungen, 2016, Teil I S. 78.

den einzelne (Kunden-)Daten oder Datenpakete entweder zwischen Unternehmen verkauft bzw. gekauft oder diese werden dem Unternehmer von Nutzern im Rahmen der Inanspruchnahme einer IT-Dienstleistung, etwa eines sozialen Netzwerks, zur Verfügung gestellt (*Tauschwert* von Daten).[70]

Der Gebrauchs- und Tauschwert von Daten rechtfertigt es, ihnen einen Warencharakter zuzuschreiben.[71] Die Annahme eines Warencharakters von Daten findet ihre Bestätigung ebenso in Erwägungsgrund 13 des Vorschlags einer Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte vom 09. Dezember 2015 (siehe zu diesem Richtlinienvorschlag ausführlich unter 6.2.): [72]

In der digitalen Wirtschaft haben Informationen über Einzelpersonen für Marktteilnehmer immer mehr einen mit Geld vergleichbaren Wert. Digitale Inhalte werden häufig nicht gegen Zahlung eines Preises bereitgestellt, sondern gegen Erbringung einer anderen Leistung als Geld, d. h. durch Gewährung von Zugang zu personenbezogenen oder sonstigen Daten.

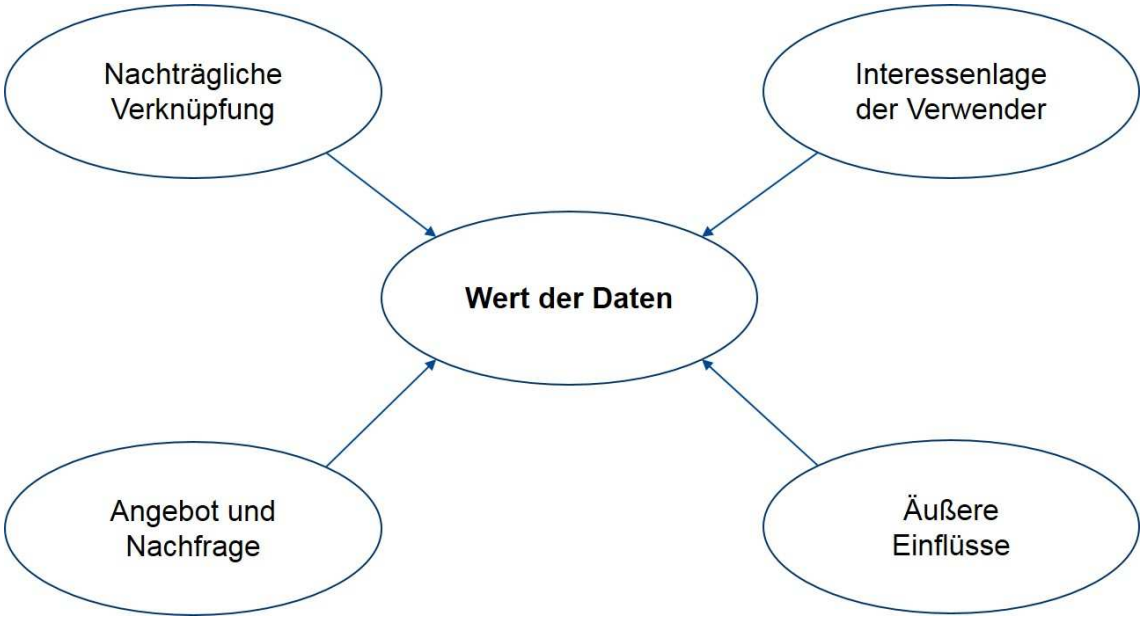
Diese Wertung steht auch im Einklang mit deutschem Verfassungsrecht. Das aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 des Grundgesetzes (GG) folgende allgemeine Persönlichkeitsrecht, aus dem auch das Recht auf informationelle Selbstbestimmung abgeleitet wird, hat neben einer ideellen auch eine vermögensrechtliche Qualität. Der Europäische Gerichtshof für Menschenrechte (EGMR),[73] der Europäische Gerichtshof (EuGH),[74] das Bundesverfassungsgericht (BVerfG)[75] und der Bundesgerichtshof (BGH)[76] haben dies einhellig bestätigt. In der juristischen Literatur wird diese Auffassung dagegen fast überwiegend abgelehnt.[77]

Doch den konkreten Wert eines einzelnen Datums oder auch nur bestimmter Datenkategorien zu bestimmen, erweist sich als große Schwierigkeit und häufig sogar als unmöglich. Dies ist im Wesentlichen vier Faktoren geschuldet, die allesamt Einfluss auf den Wert der Daten haben:

---

[70] Vgl. Wandtke, MMR 2017, 6, 7.
[71] Wandtke, MMR 2017, 6, 7.
[72] COM(2015) 634 final; vgl. ebenso Spindler, MMR 2016, 147 ff.
[73] EGMR, Urt. v. 19.02.2015 – 53649/09 – NJW 2016, 781.
[74] EuGH, Urt. v. 13.05.2014 – C-131/12 – MMR 2014, 455.
[75] BVerfG, Beschl. v. 22.08.2006 – 1 BvR 1168/04 – WRP 2006, 1361.
[76] BGH, Urt. v. 01.12.1999 – I ZR 49/97 – NJW 2000, 2195; BGH, Urt. v. 31.05.2012 – I ZR 234/10 – GRUR 2013, 196.
[77] Vgl. hierzu etwa Schack, AcP 195 (1995), 594 ff.

Abbildung 2
Einflussfaktoren auf den Wert der Daten



Quelle: Eigene Darstellung

– Zunächst ist der Wert eines Datums von der (nachträglichen) Verknüpfung mit weiteren Daten und Informationen abhängig.[78] Ein Problem besteht somit darin, dass derjenige, der seine Daten als Gegenleistung weitergibt, bei Vertragsschluss noch nicht abschätzen kann, welchen Wert seine Daten durch eine eventuelle Verknüpfung mit anderen Daten noch erhalten werden.

Beispiel

Der bloße Name einer Person stellt an sich – sofern es sich nicht von vornherein um eine prominente Person des öffentlichen Lebens handelt – ein bloß neutrales Datum dar. Erst durch die Verknüpfung mit weiteren Daten, wie beispielsweise Alter, Ausbildung, berufliche Erfolge, Kreditwürdigkeit oder persönliche Interessen, wird das Datum „Name“ durch weitere Informationen angereichert, die eine Wertsteigerung zur Folge haben können.[79]

[78] Bisges, MMR 2017, 301, 302.
[79] Bisges, MMR 2017, 301, 302.

Möchte z. B. ein Online-Shop gezielt Werbung schalten, so hat alleine der Name einer Person hierfür nur einen geringen wirtschaftlichen Wert. Ist dagegen bekannt, dass sich die betreffende Person genau für das Warensortiment des Online-Shops interessiert und auch finanziell gut gestellt ist, steigt die Bedeutung für den Online-Shop. Eine weitere Steigerung erfolgt etwa dann, wenn noch konkrete Kaufabsichten der betreffenden Person hinzukommen.

Weiterhin kann ihr Nutzen für verschiedene „Verwerter" zwischen völliger Wertlosigkeit und enormer Kostbarkeit variieren. Denn der Wert der Daten ist für jedes Unternehmen je nach seinen Interessen anders zu bestimmen.

Beispiel

Die Kenntnis über die persönlich bevorzugte Automarke einer Person hat für ein Autohaus einen sehr großen Wert. Auch für einen Buchladen kann eine derartige Kenntnis von Vorteil sein, da der betreffenden Person Literatur über die bevorzugte Automarke angeboten werden kann. Ist jedoch bekannt, dass die betreffende Person keine Bücher liest, so sinkt der Wert für den Buchladen gegen Null.

– Hinzu treten weitere äußere Umstände, die die Marktmechanismen von Angebot und Nachfrage beeinflussen und so den Wert der Daten im Laufe der Zeit schwanken lassen. Auch die persönlichen Daten wie beispielsweise das Gesicht, die Stimme, das Geschlecht oder der Name, unterliegen den gleichen Bedingungen von Angebot und Nachfrage wie andere Waren. Ihre Kommerzialisierung erfolgt als „unkörperliche Waren".[80]

Beispiel

Angebot und Nachfrage können auch durch verschiedene Trends beeinflusst werden. Ein derzeit weit verbreiteter Trend ist das sog. Self-Tracking. Beim „vermessenen Ich"[81] werden mithilfe von mit Sensoren ausgestatteten Armbändern verschiedenste Körper- und Aktivitätsdaten wie beispielsweise der Pulsschlag, der Blutdruck, die Anzahl der aufgenommenen Kalorien oder die Zahl der gelaufenen Kilometer sowie die Schlafdauer aufgezeichnet und anschließend auch häufig in sozialen Netzwerken und auf Online-Plattformen mit anderen geteilt. Werden diese Daten hierdurch von den Nutzern freiwillig gesammelt und anschließend preisgegeben, so führt dies zu einer Erhöhung der Angebotskurve am Datenmarkt.

---

[80] Wandtke, MMR 2017, 6, 8.
[81] Vgl. Self-Tracking – Das vermessene Ich, abrufbar unter: http://www.wissen.de/self-tracking-das-vermessene-ich, zuletzt abgerufen am 13.06.2017.

– Nicht zuletzt spielen Faktoren wie der Erlass neuer gesetzlicher Regelungen oder Ereignisse, die unter Umständen auch das Nutzerverhalten beeinflussen können, eine nicht zu unterschätzende Rolle.

Beispiel

Ein Beispiel für gesetzliche Neuregelungen, durch die sich der Wert bestimmter Daten verändert hat, sind die durch das IT-Sicherheitsgesetz eingefügten Meldepflichten bei Datenschutzverstößen von Betreibern Kritischer Infrastrukturen (§ 8b BSIG; siehe hierzu im Einzelnen unter 8.). Durch diese hat sich der Wert meldepflichtiger Daten über IT-Sicherheitsverstöße um ein Vielfaches erhöht, nachdem vor allem Mitbewerber ein besonderes Interesse hieran haben können, resultieren derartige Verstöße jedoch häufig in einem immensen Reputationsverlust des betroffenen Unternehmens.

Zusammenfassend bereitet die Bestimmung eines präzisen Werts von Daten erhebliche Schwierigkeiten, doch muss im Hinblick auf die oben genannten faktischen und rechtlichen Umstände das „Ob“ eines wirtschaftlichen Wertes und damit auch ein Warencharakter von Daten bejaht werden. Dass dies der Fall ist, zeigt der bereits stark vertretene Handel mit Nutzerdaten. Hier werden beispielsweise Daten durch Zwischenhändler erhoben, gesammelt und zu Datenpaketen zusammengefasst, die dann an Interessenten weiterverkauft werden. Die Web-Daten deutscher Internetnutzer werden beispielsweise ab ca. 10.000 EUR monatlicher Gebühr auf dem Datenmarkt angeboten.[82]

Kommt Daten ein bestimmter Wert zu, so stellt sich in diesem Zusammenhang als nächstes die Frage, wie die Bezahlung mit Daten rechtlich einzuordnen ist.
.

[82] Vgl. Eckert/Klofta/Strozyk, Handel mit Nutzerdaten – Milliardengeschäft mit ausgespähten Daten, v. 01.11.2016, abrufbar unter: https://www.tagesschau.de/inland/tracker-online-101.html, zuletzt abgerufen am 14.06.2017.

6 Wie ist die Bezahlung mit Daten rechtlich einzuordnen?

Umstände des Einzelfalls entscheidend

Bei der Frage, wie die Bezahlung mit Daten rechtlich einzuordnen ist, spielen neben dem geltenden nationalen Recht auch europäische Regulierungsansätze eine Rolle. Bislang handelt es sich jedoch bei letztgenannten nur um Vorschläge, zu einer Einigung über die in Rede stehenden Rechtsakte ist der europäische Gesetzgeber noch nicht gelangt.

6.1 Nationales Recht: Bürgerliches Gesetzbuch (BGB)

Grundsätzlich gilt im deutschen Vertragsrecht der Grundsatz der Vertragsfreiheit. Dieser beinhaltet zum einen das Recht, frei zu bestimmen, ob und mit wem ein Vertrag abgeschlossen werden kann (Abschlussfreiheit), zum anderen das Recht, den Inhalt des Vertrags frei zu bestimmen (*Gestaltungsfreiheit*).[83] Das Gesetz gibt verschiedene Vertragstypen vor, deren Regelungen einer interessengerechten Durchführung des Vertragsverhältnisses dienen sollen.[84]

Beispiele

Kaufvertrag, §§ 433 ff. BGB; Darlehensvertrag, §§ 488 ff. BGB; Mietvertrag, §§ 535 ff. BGB; Werkvertrag, §§ 631 ff. BGB; Dienstvertrag, §§ 611 ff. BGB

6.1.1 Zugrundeliegender Vertragstyp

Aufgrund des Grundsatzes der Vertragsfreiheit ist es schon nach derzeitiger Rechtslage möglich, Rechtsgeschäfte unter Verwendung von Daten abzuschließen. Nicht abschließend geklärt ist dabei aber, ob die Gegenleistung, z. B. für die Bereitstellung digitaler Güter, wie E-Books, Musik etc., tatsächlich nur die Hingabe von Daten ist, oder aber auch die Erklärung der datenschutzrechtlichen Einwilligung. Letzteres liegt bereits deshalb nahe, weil die Einwilligung in der Regel erforderlich ist, um personenbezogene Daten unter Einhaltung des Datenschutzrechts verarbeiten zu dürfen. Es sprechen daher gute Gründe dafür, dass auch die Erklärung der Einwilligung als vertragliche Gegenleistung geschuldet ist.

[83] Musielak/Hau, in: Musielak/Hau, Grundkurs BGB, 4. Aufl. 2015, Rn. 128 f.
[84] Musielak/Hau, in: Musielak/Hau, Grundkurs BGB, 4. Aufl. 2015, Rn. 131.

Ist die Einwilligung aber ebenfalls als Gegenleistung geschuldet, so handelt es sich gerade nicht um einen Tauschvertrag gem. § 480 BGB („Daten gegen Leistung“), sondern um einen Vertrag mit doppeltem Typus. Das bedeutet, dass auf die Zurverfügungstellung des Leistungsgegenstands und auf die Erklärung der datenschutzrechtlichen Einwilligung die jeweils passenden vertraglichen Vorschriften Anwendung finden.

Für die unternehmensseitig geschuldete Leistung sind dabei verschiedene Fallkonstellationen denkbar. Es kann beispielsweise ein Vertrag über die punktuelle und endgültige Überlassung eines digitalen Inhaltes, z. B. eines E-Books, geschlossen werden oder auch über die dauerschuldvertragliche Bereitstellung der Nutzungsmöglichkeit von Social Media oder anderen Unternehmensplattformen. Diese Leistungen lassen sich zumindest dann kaufvertragsrechtlich beurteilen, wenn die endgültige Überlassung des Leistungsgegenstands geschuldet ist. Denn die endgültige, punktuelle Überlassung eines Gegenstands entspricht auch dann dem Leitbild des Kaufvertragsrechts, wenn ein sonstiger Gegenstand überlassen wird, der gerade keine Sache ist. Dies folgt unmittelbar aus § 453 Abs. 1 BGB.

Als Gegenleistung kommen die Überlassung von Daten und die Erklärung der Einwilligung allein oder in Kombination mit der Zahlung eines (dann reduzierten) Entgelts in Betracht. Die Erklärung der Einwilligung ähnelt dabei der Einräumung von Nutzungsrechten in einem Lizenzvertrag. Sie beurteilt sich nach überwiegender Ansicht daher nach den Vorschriften des Miet- und Pachtvertragsrechts. Auswirkungen hat dies vor allem auf die Frage, was geschieht, wenn die Einwilligung widerrufen wird. Dies ist nach deutschem und europäischem Datenschutzrecht jederzeit möglich (vgl. hierzu ausführlich unter 6.1.4.).

6.1.2 Festlegung der wesentlichen Vertragsinhalte

Für die Wirksamkeit eines Vertrags ist es erforderlich, die sog. „essentialia negotii“ festzulegen. Durch diese wird der wesentliche Vertragsinhalt festgeschrieben. Die essentialia negotii umfassen die beiden Parteien des Vertrags und die gegenseitigen Hauptleistungspflichten. Der Vertrag kommt erst durch die Einigung beider Vertragsparteien zustande. Für offene oder versteckte Einigungsmängel sieht das Gesetz in den §§ 154, 155 BGB gewisse Regelungen vor, etwa dass der Vertrag als nicht geschlossen angesehen wird.

Beispiel

Bei einem Kaufvertrag über ein Kraftfahrzeug beinhalten die essentialia negotii die Identität des Käufers und des Verkäufers, die genaue Bezeichnung des Kraftfahrzeugs und die Festsetzung der Höhe des Kaufpreises als Gegenleistung. Die Festsetzung der Höhe des Kaufpreises kann jedoch auch im Nachhinein aufgrund konkret festgelegter Kriterien erfolgen.

Werden personenbezogene Daten sowie die Erklärung der datenschutzrechtlichen Einwilligung als Gegenleistung eingesetzt, so zählt die Bestimmung der betroffenen Daten ebenso zu den „essentialia negotii“. Da eine Einigung über die Gegenleistung erzielt werden muss, ist es erforderlich, dass diese als wesentlicher Vertragsbestandteil detailliert beschrieben wird. Dies folgt für personenbezogene Daten im Übrigen auch aus dem Datenschutzrecht.

Hier stellen sich jedoch vor allem praktisch höchst relevante Fragen: Ist es erforderlich, dass jedes einzelne Datum, das übertragen wird, genau aufgeführt wird? Oder genügt auch eine Sammelbezeichnung von Daten? Insoweit besteht aber das Risiko, dass hinsichtlich der Abrede der beiden Parteien Einigungsmängel vorliegen, die unter Umständen dazu führen können, dass der Vertrag als nicht geschlossen anzusehen ist (§ 154 BGB). Die Auflistung jedes einzelnen Datums stellt allerdings einen erheblichen Aufwand für beide Parteien dar, sofern es sich um eine Vielzahl von Daten handeln soll. Soll der Vertrag dagegen nur wenige einzelne Daten beinhalten, gestaltet es sich hier leichter, alle Daten einzeln im Vertrag aufzulisten. Ob ein Vertrag über nur wenige einzelne, präzise aufzulistende Daten in der Praxis jedoch häufig vorkommen wird, darf bezweifelt werden.

Hier zeigt sich, dass mitunter bereits bei der Festlegung des Vertragsinhalts Probleme auftreten können, sofern Daten als Gegenleistung verwendet werden.

Überdies problematisch ist die Festlegung des Verarbeitungszwecks, die ebenfalls erfolgen muss, wenn Daten und Einwilligung als Gegenleistung hingegeben werden. Die datenschutzrechtlichen Vorgaben müssen hier auf das zugrundeliegende Schuldverhältnis durchschlagen. Gerade bei Big-Data-Anwendungen wird dieser Verarbeitungszweck in der Regel zumindest dann nicht vorab bestimmt, wenn nach bisher unbekannten Zusammenhängen zwischen den Daten gesucht werden soll und noch nicht absehbar ist, für welchen Zweck dies erfolgen soll. Dies birgt das Risiko, gegen den Zweckbindungsgrundsatz zu verstoßen. Eine Möglichkeit, Big-Data-Analysen ohne Verstoß gegen das Datenschutzrecht durchzuführen, ist die vorherige explizite Begrenzung auf einen präzise angegebenen Zweck, der dann auch eingehalten wird.

Ob auch im Übrigen eine Datenschutzkonformität hergestellt werden kann, ist derzeit noch nicht abschließend geklärt. Eine Lösung, die sich juristisch aber noch durchsetzen muss, könnte sein: Der Dienstleister, der für seine Big Data Analysen um Zustimmung zur Datenverarbeitung bittet, erklärt sein Vorgehen in transparenter Weise, zeigt dabei auch mögliche Verarbeitungszwecke – notfalls auf einer höheren Abstraktionsebene – auf und gibt bestimmte Verfahrensgarantien, etwa eine Löschung der Daten für den Fall, dass in absehbarer Zeit keine Verwertbarkeit in dem abgesteckten Rahmen sichtbar wird. Die Einwilligung müsste in diesem Fall eindeutig mit der Maßgabe erfolgen, dass der Betroffene sich mit der Big Data Analyse trotz der notwendig abstrakteren Zwecksetzung einverstanden erklärt. Ein solches Vorgehen wäre natürlich nur dort zulässig, wo eine konkretere Zwecksetzung zunächst nicht möglich ist (um einen Missbrauch durch Verschleierung von Geschäftszwecken zu vermeiden). Die durchaus weitreichende Möglichkeit der Zweckänderung, wie sie nunmehr Art. 6 Abs. 4 DS-GVO

vorsieht, spricht ebenfalls für die hier vertretene Auffassung. Sie erinnert an eine „fair use“-Regelung und verpflichtet die verantwortliche Stelle zu einer Abwägung unter Berücksichtigung der Interessen des Betroffenen (Folgenabschätzung, Nutzung von Schutzinstrumenten wie Verschlüsselung oder Pseudonymisierung etc.).

6.1.3 Rückabwicklung des Vertrags bei Rücktritt des Datenschuldners

Die uneingeschränkte Vervielfältigbarkeit der Daten stellt auch bei den Gewährleistungsrechten, insbesondere bei dem Rücktritt, ein großes Problem dar. Nach erfolgtem Rücktritt wird das Vertragsverhältnis in ein sog. Rückgewährschuldverhältnis umgewandelt (§ 346 BGB). Dies bedeutet, dass die gegenseitig gewährten Leistungen einander zurück zu gewähren sind. Wie dies im Falle von Daten aussehen soll, ist bisher ungeklärt. Insbesondere die Frage, ob für eine Rückabwicklung die bloße Löschung genügt oder auch die Herausgabe der Daten geschuldet ist, ist weder in Rechtsprechung, noch in der Literatur entschieden. Da im Rahmen des Rückgewährschuldverhältnisses der Status vor Abschluss des Rechtsverhältnisses herzustellen ist, wird eine Löschung in der Regel ausreichen. Daneben besteht allerdings nach der Datenschutzgrundverordnung auch ein Herausgabeanspruch gem. Art. 15 DSGVO, der unabhängig von einem Rückgewährschuldverhältnis bestehen kann.

Große Schwierigkeiten bei der tatsächlichen Umsetzung dieser Rücktrittsfolgen ergeben sich, wenn die vom Vertragspartner als Gegenleistung erhaltenen Daten bereits mit anderen Daten verknüpft und weiterverarbeitet wurden:

- Das Rücktrittsrecht enthält mit einem Anspruch auf Nutzungsersatz die Vorgabe, dass der Gläubiger der Leistung alle Gebrauchsvorteile (§ 100 BGB), die er aus der Leistung erlangt hat, herauszugeben hat.
- Dies muss ebenso im Datenüberlassungsvertrag gelten und zwar selbst dann, wenn sich der Nutzungsersatz eigentlich auf Gebrauchsvorteile von Sachen und Rechten beschränkt und damit jedenfalls seinem Wortlaut nach nicht auf sonstige unkörperliche Gegenstände wie Daten anwendbar ist. Man könnte nämlich darauf abstellen, der Gebrauchsvorteil werde durch das Recht zur Nutzung der Daten erlangt. Aus Sinn und Zweck des § 346 BGB könnte sich ferner ergeben, dass auch Vorteile, die aus Daten gezogen werden, herauszugeben sind. Ebenso ließe sich darüber nachdenken, ob statt einer Löschung bzw. Herausgabe der verarbeiteten Daten ein Wertersatzanspruch geschuldet sein kann.
- Dies ist noch völlig ungeklärt. Es wäre aber wohl unverhältnismäßig, wenn der Rückgewährschuldner wegen eines einzelnen Datensatzes z. B. eine komplette Analyse auf Basis von Hunderttausenden von Daten nicht mehr nutzen dürfte (nur für künftige Berechnungen müsste natürlich der fragliche Datensatz unberücksichtigt bleiben). Hier Wertersatz zu fordern, könnte im Einzelfall auch rechtsmissbräuchlich sein.

Zur Überprüfung, ob der Datengläubiger (das datenerhebende Unternehmen) rechtmäßig mit den Daten umgeht, stehen dem Datenschuldner die Instrumentarien des Datenschutzrechts zur Verfügung (Betroffenenrechte wie Auskunft, Löschung etc.). Die

Nichteinhaltung des Datenschutzrechts wird mit hohen Geldbußen geahndet (bis zu 20 Millionen Euro oder vier Prozent des weltweit erzielten Jahresumsatzes, Art. 83 DSGVO).

6.1.4 Jederzeitige Widerruflichkeit der Einwilligung

Im Vertragsrecht gilt der Grundsatz „pacta sunt servanda“. Dies bedeutet, dass Verträge nach ihrem Abschluss grundsätzlich bindend sind und dass sich die Parteien nur aufgrund bestimmter gesetzlich geregelter Fälle wieder vom Vertrag lösen können.

Beispiel

Liegt eine arglistige Täuschung oder widerrechtliche Drohung vor, kann sich der Vertragspartner durch die wirksame Anfechtung vom Vertrag lösen (§ 123 BGB). Im Kaufrecht ist eine Lösung vom Vertrag unter bestimmten Voraussetzungen beispielsweise durch den soeben bereits erwähnten Rücktritt möglich, wenn die Ware einen Sachmangel aufweist (§§ 437 Nr. 2, 323 Abs. 1, 346 BGB).

Stellen nun Daten die Gegenleistung eines Vertrags dar, so ist die Erhebung, Verarbeitung und Nutzung dieser Daten für den Fall, dass es sich um personenbezogene Daten handelt, nur zulässig, sofern ein gesetzlicher Erlaubnistatbestand vorliegt oder der Betroffene seine Einwilligung erteilt hat (sog. Verbot mit Erlaubnisvorbehalt, § 4 Abs. 1 BDSG bzw. Art. 6 Abs. 1 DS-GVO). Wie nachfolgend im Einzelnen aufgeführt, bedarf es bei Verwendung von personenbezogenen Daten als Gegenleistung stets einer Einwilligung des Datenschuldners, damit der andere Vertragsteil diese Daten rechtskonform verwenden kann. Aus der Tatsache, dass eine solche Einwilligung stets frei widerruflich ist (so ausdrücklich Art. 7 Abs. 3 Satz 1 DS-GVO), resultieren in rechtlicher Hinsicht zahlreiche Probleme.

Fallbeispiel

Über die Website bandcamp.com können Musikstücke allein gegen die Zurverfügungstellung personenbezogener Daten, ergänzt um die Erklärung der datenschutzrechtlichen Einwilligung, erworben werden. Nach der Bereitstellung des Musikstückes kann die Einwilligung aber widerrufen werden, sodass der Vertragspartner gewissermaßen mit leeren Händen dasteht.

Eine Parallele besteht insoweit zu einem etwaigen berechtigten Löschungsverlangen des Kunden hinsichtlich der ihn betreffenden personenbezogenen Daten (Art. 17 DS-GVO). Datenschutzrecht und Vertragsrecht sind hier auch in den aktuellen europäischen Regulierungsvorschlägen nicht aufeinander abgestimmt.

6.1.4.1 Kein gesetzlicher Erlaubnistatbestand für die Datenverarbeitung des anderen Vertragsteils

Das Verpflichtungsgeschäft, also der zwischen dem Unternehmer und dem Verbraucher geschlossene Vertrag über die Hingabe personenbezogener Daten und die Erklärung der Einwilligung, beinhaltet die schuldrechtliche Verpflichtung zur Gestattung der Nutzung von Daten. Datenschutzrechtlich ist die Gestattung der Nutzung der Daten als Mittel für eigene Geschäftszwecke unabhängig von einer Einwilligung des Betroffenen dann zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG). Erforderlichkeit liegt dann vor, wenn die personenbezogenen Daten gerade notwendig sind, um die Pflichten aus dem Vertrag erfüllen und eigene Rechte geltend machen zu können. Maßgeblich ist hierbei die Zweckbestimmung des schuldrechtlichen Vertrags.

Grundsätzlich erfasst § 28 Abs. 1 Satz 1 Nr. 1 BDSG somit die Fälle, in denen die Daten nicht direkt das Vertragsverhältnis betreffen, sondern als Ergänzung zur ordnungs-gemäßen Begründung, Durchführung oder Beendigung erforderlich sind. Hauptkriterium ist zudem, dass die Daten gerade für eigene Geschäftszwecke erhoben werden und dass das Kriterium der Erforderlichkeit erfüllt ist.

Beispiel

Kauft man eine bestimmte Ware in einem Online-Shop, so sind für die Abwicklung des Kaufs der Name und die Anschrift des Käufers, die Art und die Menge des gekauften Artikels, die Zahlungsweise, die Versandangaben und gegebenenfalls auch die Kontoverbindung erforderlich. Daneben gibt es Daten, die nicht zwingend erforderlich sind, aber die die Abwicklung des Rechtsgeschäfts erleichtern würden, so beispielsweise die Telefonnummer. Hier ist dem Unternehmer zu empfehlen, bei der Eingabemaske zwischen Pflichtangaben, die für die Durchführung des Rechtsgeschäfts erforderlich sind, und freiwilligen Angaben, wie die der Telefonnummer, zu unterscheiden.

Sollen Daten gerade die Hauptleistung des rechtsgeschäftlichen Schuldverhältnisses als solche darstellen, so könnte auch hier eine datenschutzrechtliche Zulässigkeit der Nutzung der Daten nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG vorliegen, da die Daten hier „erst recht“ für die Durchführung des Vertrags benötigt werden. Allerdings findet § 28 Abs. 1 Satz 1 Nr. 1 BDSG seine Einschränkung in dem Grundsatz der Erforderlichkeit.

Würde man die Nutzung der Daten, die als Gegenleistung in einem vertraglichen Verhältnis festgelegt wurden, unter den gesetzlichen Erlaubnistatbestand des § 28 Abs. 1 Satz 1 Nr. 1 BDSG fassen, dann würde der Grundsatz der Erforderlichkeit gerade dadurch umgangen, dass es der Disposition der Parteien unterliegt, welche und wie viele Daten genutzt werden sollen (Gestaltungsfreiheit als Bestandteil des Grundsatzes der Vertragsfreiheit). Aus diesem Grund ist zu bezweifeln, dass § 28 Abs. 1 Satz 1 Nr. 1 BDSG auf den Fall, in dem Daten die unmittelbare Gegenleistung im Rahmen eines schuldrechtlichen Vertrags bilden, anwendbar ist.

Nach Art. 6 Abs. 1 Satz 1 lit. b DS-GVO ist die Verarbeitung von Daten unabhängig von einer Einwilligung des Betroffenen nur zulässig, wenn diese für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist. Auch hier ist das Kriterium der Erforderlichkeit zu beachten. Diese Vorschrift erfasst somit die Fälle, in denen die Daten nur gelegentlich der Vertragserfüllung, also beiläufig, verarbeitet werden. Stellt die Verarbeitung der Daten jedoch den Hauptzweck dar, nachdem diese gerade als Gegenleistung übertragen werden, so kann diese Verarbeitung nicht durch Art. 6 Abs. 1 Satz 1 lit. b DS-GVO gerechtfertigt werden. Eine Änderung dieser EU-Rechtslage in naher Zukunft ist nicht zu erwarten.

6.1.4.2 Kein pauschaler Ausschluss der Widerruflichkeit der Einwilligung

Wie aufgezeigt, bedarf der Vertragspartner zur datenschutzkonformen Verwendung der Daten in Ermangelung eines gesetzlichen Ermächtigungstatbestands stets einer Einwilligung des Datenschuldners. Nur so kann die Verpflichtung aus dem zugrundeliegenden Vertrag, die Nutzung der betreffenden Daten zu gestatten, erfüllt werden. Allerdings ist diese datenschutzrechtliche Einwilligung stets frei widerruflich (Art. 7 Abs. 3 DS-GVO). Auch ein pauschaler Verzicht hierauf ist aufgrund des Grundrechts auf informationelle Selbstbestimmung, das dem gesamten Datenschutzrecht zugrunde liegt, nicht möglich. Das Recht auf informationelle Selbstbestimmung gewährleistet die Befugnis des Einzelnen, selbst über die Preisgabe und die Verwendung seiner Daten zu bestimmen. Ein vollständiger Verlust der Möglichkeit des Widerrufs der Einwilligung würde zu einem Verlust der Bestimmungsmöglichkeit über die Daten führen und dadurch auch zu einem Verlust des Rechts auf informationelle Selbstbestimmung. Was allerdings zulässig sein müsste, ist – ähnlich wie beim Recht am eigenen Bild – ein Verzicht auf das Recht zum Widerruf der Einwilligung in bestimmten Nutzungsszenarien, solange dies nicht die weitere Verwendung der eigenen personenbezogenen Daten auch in anderen Kontexten verhindert.

6.1.4.3 Auswirkungen eines Widerrufs der Einwilligung

Welche Auswirkungen der Einwilligungswiderruf auf das zugrundeliegende Vertragsverhältnis hat, ist derzeit weder gesetzgeberisch noch gerichtlich geklärt. Auch in der Literatur wird dieses Problem nur von wenigen Autoren adressiert. Bei Zugrundelegung

der zivilrechtlichen Grundprinzipien lässt sich aber von folgenden Annahmen ausgehen: Das deutsche Zivilrecht unterscheidet zwischen einer vertraglichen Verpflichtung und dem Vollzug dieser Verpflichtung (sog. Trennungs- und Abstraktionsprinzip). Als dingliches Rechtsgeschäft ließe sich die Einwilligung begreifen, die Daten selbst werden schlicht überlassen, da sie nicht Gegenstand gesonderter Eigentumsrechte sind. Verpflichtet ein Vertrag zur Erklärung der datenschutzrechtlichen Einwilligung, so führt der Widerruf der Einwilligung dazu, dass diese Verpflichtung nicht länger erfüllt wird. Beurteilt sich die Einwilligung nach den Vorschriften des Mietvertragsrechts (vgl. hierzu bereits unter 6.1.1), so wird mit der Einwilligung gewissermaßen die „Mietsache“ nicht länger zur Verfügung gestellt, sodass der Unternehmer im Falle eines verbraucherseitigen Widerrufs der Einwilligung den Vertrag mit dem Verbraucher kündigen kann, § 543 Abs. 2 Nr. 1 BGB.

Als Rechtsfolge eines wirksamen Einwilligungswiderrufs sind die personenbezogenen Daten zu löschen. Dies folgt sowohl aus dem Datenschutzrecht, als auch aus den mietvertragsrechtlichen Vorschriften. Dem ist unbedingt Folge zu leisten, zumal nach der Datenschutz-Grundverordnung anderenfalls empfindliche Sanktionen drohen.

6.1.4.4 Missbrauchsrisiken und Lösungsszenarien

Inwieweit bei der unternehmensseitigen Leistung digitaler Inhalte dem Missbrauchsrisiko vorgebeugt werden kann, dass der Verbraucher den Inhalt bereits vervielfältigt und weitergereicht hat, ist bislang ungeklärt. Verdeutlicht werden soll dies an folgendem Fall, anhand dessen auch mögliche Lösungsoptionen ausgearbeitet werden. Deutlich sein sollte aber, dass es zu diesem Problemfeld bislang weder aus der Rechtsprechung, noch von Seiten des Gesetzgebers Lösungsangebote gibt. Das Risiko, dem die Wirtschaft hier unterliegt, ist insofern nicht unerheblich.

Fallbeispiel

Der Unternehmer A schließt mit dem Kunden K einen Vertrag über die einmalige Überlassung eines E-Books zur dauerhaften Nutzung ab. Im Gegenzug verpflichtet sich der Kunde, A bestimmte personenbezogene Daten als Gegenleistung zur Verfügung zu stellen und die datenschutzrechtliche Einwilligungserklärung zu erteilen. Nach drei Wochen widerruft K jedoch seine zuvor erteilte datenschutzrechtliche Einwilligung.

Ein bloßes Vertrauen darauf, dass der Vertragspartner von seinem Recht, die datenschutzrechtliche Einwilligung zu widerrufen, keinen Gebrauch macht, reicht zur rechtlichen Absicherung des Unternehmers nicht aus. Um den Unternehmer vor einer derartigen Fallkonstellation zu schützen, kommen insbesondere folgende Lösungsmöglichkeiten in Betracht.

– Eine Möglichkeit besteht darin, für den Fall der Verwendung von personenbezogenen Daten die Unwiderruflichkeit der Einwilligung festzusetzen. Für andere Fallgruppen des Persönlichkeitsrechts wird unter Hinweis auf das Prinzip der Rechtssicherheit und der Vertragstreue eine Unwiderruflichkeit der Einwilligung dann angenommen, wenn die Einwilligung vertraglich erteilt wurde und der Einwilligende eine Gegenleistung erhalten hat. Daher könnte die Unwiderruflichkeit der Einwilligung auch auf diesen Fall Anwendung finden. Eine derartige Unwiderruflichkeit hätte jedoch eine erhebliche Einschränkung des grundrechtlich gewährleisteten Rechts auf informationelle Selbstbestimmung und damit auch einen Verlust der Möglichkeit, selbst über den Umgang mit seinen Daten zu bestimmen, zur Folge (vgl. oben, 6.1.4.2). Einer solchen Klausel haftet daher jedenfalls in der gegenwärtigen Phase der Rechtsunsicherheit ein hohes Risiko an, als unwirksam erachtet zu werden, sodass der Verbraucher auch weiterhin ein Widerrufsrecht hat.

– Widerruft der Verbraucher nun seine zuvor erteilte Einwilligung, so kann aber möglicherweise über das Instrument schuldrechtlicher Sekundäransprüche bzw. -rechte ein Ausgleich zwischen den Interessen der Vertragsparteien geschaffen werden. Zu denken wäre hierbei beispielsweise an Kündigungs- oder Rücktrittsrechte des Datenverarbeiters oder auch Schadensersatzansprüche desselben gem. § 280 BGB bzw. § 122 BGB analog. Dadurch könnte sowohl dem informationellen Selbstbestimmungsrecht des Verbrauchers, der nach wie vor jederzeit widerrufen kann, als auch den vertraglichen Interessen des Einwilligungsempfängers Rechnung getragen werden. Voraussetzung hierfür ist allerdings, dass der Einwilligungswiderruf einen Vertragsbruch des Verbrauchers darstellt. Für Schadensersatzansprüche ist darüber hinaus das Vorliegen eines bezifferbaren Vermögensschadens notwendig. In diesem Zusammenhang wird daher gerade auch die Frage entscheidend sein, ob mit dem Datenverarbeitungsvorgang bereits begonnen wurde oder nicht.

– Dem Unternehmer könnte im Falle des Widerrufs der datenschutzrechtlichen Einwilligung ein Wertersatzanspruch zugebilligt werden. Hier stellt sich jedoch wiederum das Problem der genauen Bezifferung dieses Anspruchs. Auch könnte der Kunde aufgrund des drohenden Wertersatzanspruchs von der Ausübung seines Widerrufsrechts abgehalten werden. Da dem Verbraucher das Recht, seine Einwilligung jederzeit zu widerrufen, verbleibt, könnte die Zubilligung eines Wertersatzanspruchs aber einen zielführenden Kompromiss darstellen.

Die Auswirkungen, die eine Anerkennung von Daten als Gegenleistung im Vertrag hat, ist für die Wirtschaft erheblich. Es ist ungeklärt, welchen Regelungen derartige Verträge folgen, und welche Auswirkungen eine Nichtleistung, eine mangelhafte Leistung oder auch der Widerruf der Einwilligung in die Datenverarbeitung haben. Diese Fragen werden vielmehr gerade erst aufgeworfen. Für die Wirtschaft ergibt sich daher ein nicht unerhebliches Risiko. Andererseits handelt es sich hierbei in vielerlei Hinsicht um rechtsdogmatische Probleme, die sich in der Praxis weniger schwerwiegend darstellen könnten, als in der Theorie. Jedenfalls scheinen potenzielle zivilrechtliche Schadensersatzansprüche überschaubar. Schwerer wiegen die Vorgaben der Datenschutzgrund-

verordnung, die ganz empfindliche Bußgelder im Falle einer Verletzung des Datenschutzrechts (z. B. durch Datenverarbeitung ohne Vorliegen einer Einwilligung des Betroffenen und ohne Erlaubnistatbestand) vorsieht.

6.2 Europäische Regulierungsansätze

Zugleich mit dem Vorschlag einer Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte wurde von der EU-Kommission ein Vorschlag für eine Richtlinie über bestimmte vertragsrechtliche Aspekte des Online-Warenhandels und anderer Formen des Fernabsatzes von Waren vorgelegt. Beide Richtlinien sollen der Anpassung des Rechtsrahmens an den technischen und gesellschaftlichen Fortschritt dienen. Für die Beleuchtung der normativen Anknüpfungspunkte zu Daten als Wirtschaftsgut ist jedoch alleine die erste Richtlinie von Relevanz, da die zweite vorrangig Gewährleistungsrechte und Rechtsfolgen zum Gegenstand hat und auf die grundlegenden Aussagen der ersten Richtlinie aufbaut. Richtlinien bedürfen im Gegensatz zu Verordnungen noch stets einer Umsetzung in nationales Recht; das europäische Recht macht dabei verbindliche Vorgaben zum Ziel, nicht jedoch zu Form und Mittel der Regulierung. Verordnungen gelten dagegen unmittelbar in allen EU-Mitgliedstaaten und sind überdies in allen ihren Teilen verbindlich.

Dem EU-Richtlinienentwurf über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte vom 09. Dezember 2015 kann aus seinem Anwendungsbereich (Art. 3 Nr. 1) entnommen werden, dass die Richtlinie für alle Verträge gilt, auf deren Grundlage ein Anbieter einem Verbraucher sog. digitale Inhalte bereitstellt oder sich hierzu verpflichtet. Unter „digitale Inhalte“ fallen aus Gründen der Innovationsfreundlichkeit mit Blick auf neue Geschäftsmodelle nicht nur Daten, die in digitaler Form hergestellt und bereitgestellt werden, sondern auch Dienstleistungen (Art. 2 Nr. 1). Zugleich muss der Verbraucher als Gegenleistung einen Preis oder „aktiv eine andere Gegenleistung als Geld in Form personenbezogener oder anderer Daten erbringen“. Hieraus geht deutlich hervor, dass Daten als Gegenleistung – und mithin als Wirtschaftsgut mit Vermögenswert – eingestuft werden. Erfasst werden dabei personenbezogene Daten und andere Daten. Andere Daten sind nach dieser Richtlinie solche Daten, die keinen Personenbezug aufweisen, was im Übrigen auch die regelmäßige Unanwendbarkeit der engen datenschutzrechtlichen Vorgaben mit sich bringt (siehe hierzu gesondert unter 7.). Wie bereits dargestellt, muss der Verbraucher dem Unternehmer die Daten jedoch aktiv zur Verfügung stellen, d. h. die Richtlinie ist etwa dann nicht anwendbar, wenn die Bereitstellung über Cookies erfolgt, wie beispielsweise bei IP-Adressen (Erwägungsgrund 14). Inwieweit dies im weiteren Verfahren Bestand haben wird, wird sich zeigen.[85]

[85] So werden aktuell sowohl die aktive Bereitstellung als auch die Anwendbarkeit auf nicht personenbezogene Daten in Frage gestellt, vgl. den Bericht der Ausschusses für Binnenmarkt und Verbraucherschutz und des Rechtsausschusses vom 27.11.2017 über den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, COM(2015)0634 – C8-0394/2015 – 2015/0287(COD)

Beispiele

Unter den – wie bereits dargelegt – grundsätzlich breiten Anwendungsbereich der Richtlinie würden damit nach den Vorstellungen der Kommission neben Verträgen im B2C-Verkehr über Online-Marktplätze wie Amazon und eBay oder die Verwendung von Suchmaschinen unter Preisgabe der ei-genen Interessen anhand der Suchbegriffe sowie des eigenen Standorts auch etwa solche über die Nutzung von Cloud-Computing-Diensten, Blog-Portalen oder sozialen Netzwerken fallen, jedenfalls soweit die Zurverfügungstellung der Daten aktiv erfolgt.

Auch das Verhältnis zwischen Vertragsrecht und Datenschutzrecht ist auf europarechtlicher Ebene von Relevanz. Nach Art. 3 Nr. 8 des Vorschlags einer Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte bleibt der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten von der Online-Inhalte-Richtlinie unberührt. Dabei stellt sich die Frage, ob dies den Tatsachen entspricht und welche Konsequenzen datenschutzrechtliche Vorgaben für diesen Richtlinienvorschlag haben. Bereits an dieser Stelle ist auf das Problem hinzuweisen, dass das Datenschutzrecht in seiner Grundkonzeption gerade nicht auf die privatautonome Disposition über personenbezogene Daten ausgerichtet ist (vgl. unter 7.). Welche Auswirkungen dies auf die Entwicklung des Vorschlags der Richtlinie haben wird, der primär eine zivilrechtliche (und wettbewerbsrechtliche) Intention aufweist, bleibt abzuwarten.

Art. 13 des Richtlinienvorschlags widmet sich den möglichen Rechtsfolgen einer Vertragsbeendigung. So hat die Beendigung des Vertrags durch den Verbraucher zur Folge, dass der Anbieter alle Maßnahmen zu ergreifen hat, die erwartet werden können, um die Nutzung der ihm zur Verfügung gestellten Daten zu unterlassen (Art. 13 Abs. 2 lit. b der Richtlinie). Wie diese Unterlassung der Nutzung der Daten kontrolliert werden kann, lässt jedoch auch der Richtlinienentwurf offen. In Betracht kommt hier das Sanktionsinstrumentarium der Datenschutz-Grundverordnung (vgl. hierzu ausführlich bereits unter 1.4).

Am 07. November 2016 haben der Ausschuss für Binnenmarkt und Verbraucherschutz sowie der Rechtsausschuss des Europäischen Parlaments den Entwurf eines Berichts zu diesem Richtlinienvorschlag herausgegeben. In diesem Bericht werden der Vorschlagstext der Europäischen Kommission und eine vorgeschlagene, geänderte Version gegenübergestellt. Nach letzterer sollen personenbezogene Daten oder sonstige Daten explizit als Gegenleistung aufgenommen werden:

Diese Richtlinie gilt für alle Verträge, auf deren Grundlage ein Anbieter einem Verbraucher gegen Zahlung eines Preises und/oder als Gegenleistung für personenbezogene Daten oder andere Daten, die der Verbraucher bereitstellt oder der Anbieter oder ein Dritter im Interesse des Anbieters erfasst, digitale Inhalte oder digitale Dienstleistungen bereitstellt oder sich zur Bereitstellung verpflichtet.

Dies kommt auch in der geänderten Version des Erwägungsgrunds 13 des Richtlinienentwurfs zum Ausdruck:

In der digitalen Wirtschaft haben Informationen über Einzelpersonen für Markt-teilnehmer immer mehr einen mit Geld vergleichbaren Wert. Digitale Inhalte und digitale Dienstleistungen werden häufig nicht gegen Zahlung eines Preises bereitgestellt, sondern gegen Daten, d. h. durch Gewährung von Zugang zu personenbezogenen oder sonstigen Daten.

In seiner Stellungnahme vom 14. März 2017 problematisierte der europäische Datenschutzbeauftragte gerade den Anwendungsbereich der Richtlinie auf Daten als Gegenleistung. Er warnt ausdrücklich vor der Einführung eines solchen Konzepts, da Daten gerade nicht als bloße Waren angesehen werden können. Am 20. März 2017 veröffentlichte der Rat der Europäischen Union einen Sachstandsbericht nach der ersten Lesung über den Richtlinienentwurf, am 17. April 2017 wurden weitere Änderungsvorschläge in einer Notiz festgehalten.

Der deutsche Bundesrat begrüßt die Bestrebungen der Europäischen Kommission, Verträgen über die Bereitstellung digitaler Inhalte einen stabilen Rechtsrahmen zu verleihen. Seiner Auffassung nach sollten jedoch zuerst die grundlegenden Fragen zu „Daten als Gegenleistung“ geregelt werden, bevor das Konzept in eine Richtlinie über ein verbraucherschützendes Vertragsrecht eingeführt wird. Hierbei ist besonders problematisch, wie Rückgewähr und Wertersatzansprüche des Verbrauchers festgelegt werden sollen. Auch insgesamt wird der Richtlinienentwurf in der rechtswissenschaftlichen Literatur vor allem deswegen teils stark kritisiert, weil im deutschen Vertragsrecht die Bereitstellung digitaler Inhalte keinen eigenständigen Vertragstypus bildet und die Einwilligung als Gegenleistung aufgrund ihrer datenschutzrechtlichen Determination jedenfalls nicht ohne die gezeigten Komplikationen in das deutsche Zivilrecht umgesetzt werden kann. Eine verbindliche Rechtssetzung in Form der Verabschiedung (und anschließender Umsetzung) einer derartigen EU-Richtlinie über die Bereitstellung von Online-Inhalten wird daher sicherlich noch einige Zeit in Anspruch nehmen.

Auswirkungen für bayerische Unternehmen

Der Richtlinienentwurf sieht vor, dass Daten keinen vollumfänglichen Geldersatz darstellen sollen, sondern nur im Bereich digitaler Inhalte als Gegenleistung infrage kommen. Zudem wird sich der personelle Anwendungsbereich der Richtlinie nur auf Verträge zwischen Unternehmern und Verbrauchern beschränken, wodurch unternehmerische Daten als Gegenleistung bzw. Zahlungsmittel gerade nicht erfasst sind. Dennoch zeigen die Regulierungsansätze, dass die Thematik auf europäischer – und aufgrund des gewählten Regelungstyps einer Richtlinie zugleich auf nationaler Ebene – Berücksichtigung findet. Dabei soll diese jedoch gerade nicht den – vor allem im unternehmerischen Kontext in Bezug auf die Industrie 4.0 – immer wichtiger werdenden Bereich der „Interaktion von Maschinen“ betreffen (vgl. Erwägungsgrund 17 des Richtlinienentwurfs über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte).

7 Welche Vorgaben ergeben sich aus dem Datenschutzrecht?

Eine weitere Gretchenfrage der digitalen Wirtschaft

Nicht nur dem Anbieter des „Gartenteich-Konfigurators“ mit Preisnachlass, bei dem die Daten des Käufers (auch) zum Vertragsgegenstand werden, stellen sich datenschutzrechtliche Herausforderungen. Auch der Verkäufer beim „klassischen“ Vertrieb des Pools über einen Online-Shop könnte sich beispielsweise überlegen, ob er dem Käufer via E-Mail-Newsletter oder Telefonanruf nach ein paar Monaten ein Zubehör- oder Ersatzteil anbieten darf. Dies zeigt, dass im Rahmen der hier maßgeblichen Beleuchtung von Daten als Wirtschaftsgut der klare Fokus auf den Kundendaten liegt. Daneben stellen sich – insbesondere im Kontext der Industrie 4.0[86] – noch zahlreiche Fragen mit Blick auf die Daten von Beschäftigten.

Seit dem 25. Mai 2018 gilt allgemein und unmittelbar als europäischer Rechtssetzungsakt in Form einer Verordnung die Europäische Datenschutz-Grundverordnung (DS-GVO). Das deutsche BDSG wurde mittels des am 27. April 2017 beschlossenen Datenschutz-Anpassungs- und Umsetzungsgesetzes[87] einer umfassenden Novellierung unterzogen, die geänderten inhaltlichen Regelungen im BDSG-neu treten zeitgleich mit der DS-GVO in Kraft.

Unter anderem enthält die DS-GVO explizit die Grundsätze *Privacy by design* und *Privacy by default*, was neben der Implementierung datenschutzrechtlicher Voreinstellungen schon während des Produktionsprozesses zur Berücksichtigung des Datenschutzrechts zwingt („Datenschutz durch Technikgestaltung“, vgl. Art. 25 DS-GVO). Weicht ein Produkt von den datenschutzrechtlichen Vorgaben ab, kann dies als Sachmangel gewertet werden, da es in diesem Fall nicht dem Stand der Technik entspricht (zu den Querbeziehungen der unterschiedlichen Regelungsmaterien siehe ausführlich unter Kapitel 9.).

Werden Kundendaten als ökonomisch bedeutsame Gegenleistung angesehen, stellt sich in datenschutzrechtlicher Hinsicht das Problem, dass das Datenschutzrecht in sei-

[86] Hornung/Hofmann, Rechtsfragen bei Industrie 4.0: Rahmenbedingungen, Herausforderungen und Lösungsansätze, in: Reinhart, Handbuch Industrie 4.0, 2017, S. 191, 204.
[87] Weitere Informationen unter: http://www.bundestag.de/dokumente/textarchiv/2017/kw17-de-datenschutz/501684, zuletzt abgerufen am 29.05.2017.

ner Grundkonzeption gerade nicht auf die privatautonome Disposition über personenbezogene Daten ausgerichtet ist. Viele datenschutzrechtliche Grundsätze und zentrale Bestimmungen laufen dieser privatautonomen Disposition eher entgegen:[88]

– Der *Grundsatz der Zweckbindung* besagt dabei zunächst, dass die Verarbeitung der Daten nur für die Zwecke erfolgen darf, für die sie auch erhoben wurden. Daher muss der Zweck auch bereits bei Abschluss des Vertrags festgelegt sein. Das kann vor allem bei Big-Data-Auswertungen und -Analysen, bei denen sich der Zweck gerade erst durch die massenhafte Ansammlung von Daten formt, zu Konflikten führen.[89] Dies gilt ebenso mit Blick auf das *Prinzip der Datensparsamkeit* bzw. *Datenminimierung*, wonach die personenbezogenen Daten auf das für den jeweiligen Verarbeitungszweck notwendige Maß beschränkt sein müssen. Angesichts der bereits erwähnten Maximalhöhe der Sanktionen (Art. 83 Abs. 5 lit. a DS-GVO) sind diese Beschränkungen umso relevanter.

– Greift für die jeweiligen datenschutzrechtlich relevanten Handlungen kein spezifischer Erlaubnistatbestand und führen auch allgemeine Interessenabwägungsgesichtspunkte nicht zur Zulässigkeit der datenschutzrechtlich relevanten Vorgänge, sind hierfür nach dem sog. Verbot mit Erlaubnisvorbehalt die *Einwilligungen* der Kunden erforderlich. Diese müssen zu ihrer Wirksamkeit zahlreiche Voraussetzungen erfüllen, welche im Einzelnen wiederum Probleme bereiten können:

  - Zunächst muss eine datenschutzrechtliche Einwilligung stets freiwillig sein. Nach der DS-GVO ist bei der Beurteilung der Freiwilligkeit der Einwilligung in größtmöglichem Umfang zu berücksichtigen, ob die Erfüllung des Vertrags von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die grundsätzlich nicht für die Erfüllung des Vertrags erforderlich sind (vgl. Art. 7 Abs. 4 DS-GVO). Damit sieht die DS-GVO ein Koppelungsverbot vor. Dieses soll vor allem für die Konstellationen gelten, in denen eine Einwilligung in die Datenverarbeitung nicht erteilt werden muss, aber der Betroffene bei Verweigerung der Einwilligung auch keinen Vertrag abschließen kann.[90] Das Koppelungsverbot hat daher die Funktion, die Transparenz zu gewährleisten.[91]

[88] Specht, Ordnung der Wissenschaft 2 (2017), S. 121, 126.
[89] Vgl. hierzu weiterführend: Heckmann, in: vbw-Studie: Big Data im Freistaat Bayern - Chancen und Herausforderungen, 2016, Teil II.
[90] Buchner, DuD 2010, 39, 41.
[91] Schmidt-Kessel, ZfPW 2017, 84, 91.

Beispiel

Die Teilnahme an einem Gewinnspiel unter der Bedingung, dass der Teilnehmende in den Erhalt von Werbung des Veranstalters einwilligt, ist zukünftig nach der DS-GVO nicht mehr zulässig.

- Allerdings greift das Koppelungsverbot nach einer gut begründeten Ansicht nicht, wenn die Daten als Hauptleistung eines Vertrags festgesetzt werden, da eine gerade offene Vereinbarung der Daten als Gegenleistung von dem Zweck des Koppelungsverbots, Transparenz zu gewährleisten, nicht erfasst wird.[92]

- Weiterhin muss der Kunde eine *informierte* Einwilligung abgeben können. Dabei ist jedoch insbesondere zu berücksichtigen, dass die Daten – wie bereits dargestellt – oft erst durch deren Verknüpfung mit anderen Daten einen besonderen Wert erlangen.

– Auch unterscheiden sich Daten im Hinblick auf ihre Empfindlichkeit. Nach der sog. Sphärentheorie lassen sich Daten in drei Kategorien einteilen: Die Intimsphäre, die Privatsphäre und die Sozialsphäre, auch Öffentlichkeitssphäre genannt.[93] Während die Intimsphäre den Kernbereich privater Lebensgestaltung umfasst, betrifft die Sozialsphäre die Teilnahme am sozialen Leben. Die Privatsphäre nimmt dagegen eine Zwischenstellung zwischen den beiden anderen Sphären ein.[94]

  - Die Hingabe von Sozialdaten ist daher weit weniger einschneidend als die Hingabe von Intimdaten. Jedoch stellte das Bundesverfassungsgericht fest, dass unter den Bedingungen der modernen Datenverarbeitung diese traditionelle Sphärentheorie nicht mehr ausreichend ist. Die schnellen Datenverarbeitungsvorgänge führen dazu, dass auch „harmlose“ Daten aus der Sozialsphäre aufgrund der nachträglichen Verknüpfung sensible Informationen über den Betroffenen preisgeben können.[95]

  - Daher kann die nachträgliche Verknüpfung der Daten auch die Einordnung bezüglich der Empfindlichkeit der Daten verändern. Dieser Aspekt erschwert ebenso die Abgabe einer informierten Einwilligung durch den Betroffenen.

– Darüber hinaus ist die Einwilligung stets *frei widerruflich* (Art. 7 Abs. 3 DS-GVO), hierauf kann der Datenschuldner auch nicht wirksam verzichten. Stellen Daten jedoch nunmehr die Gegenleistung eines Vertrags dar und wird die Einwilligung nachträglich widerrufen, stellt sich die Frage, wie mit dieser „nachträglichen Nichterfüllung“[96] umgegangen werden muss (siehe hierzu bereits unter 6.1.4.).

---

[92] Schmidt-Kessel, ZfPW 2017, 84, 91.
[93] Manssen, Staatsrecht II – Grundrechte, 13. Aufl. 2016, § 11 Rn. 263.
[94] Epping, Grundrechte, 6. Aufl. 2015, Kap. 13 Rn. 629.
[95] Hufen, Staatsrecht II – Grundrechte, 5. Aufl. 2016, § 12 Rn. 4.
[96] Specht, Ordnung der Wissenschaft 2 (2017), S. 121, 126.

Auswirkungen für bayerische Unternehmen

Das Datenschutzrecht ist direkter Ausfluss aus der grundrechtlich garantierten informationellen Selbstbestimmung. Mitunter können datenschutzrechtliche Bestimmungen dazu führen, dass der wirtschaftliche Wert von Daten zugunsten der informationellen Selbstbestimmung zumindest nicht vollends ausgeschöpft werden kann. Ein transparenter und verantwortungsvoller Umgang mit Daten kann demgegenüber jedoch auch Wettbewerbsvorteile für Unternehmen mit sich bringen. Überdies besteht die Möglichkeit, durch Lösung des Personenbezugs (etwa durch effektive Anonymisierungs- oder Aggregationsverfahren[97]) die Geltung der engen Datenschutzvorgaben schon von vornherein auszuschließen.

Die seit dem 25. Mai 2018 geltende DS-GVO gibt dem Unternehmer mit der Möglichkeit der Rechtfertigung von Datenverarbeitungshandlungen über eine allgemeine Interessenabwägung ein weiteres, durchaus praxisgerechtes Instrument an die Hand. Nach Ansicht des Bayerischen Landesamts für Datenschutzaufsicht können Dienstleistungsangebote, bei denen die Gegenleistung des Nutzers in der Preisgabe von Daten besteht (beispielsweise bei einem kostenlosen E-Mail-Account) hierüber gerechtfertigt werden, sofern dies bei Vertragsabschluss klar dargestellt wird.[98] Eine Einwilligung wäre in diesem Fall nicht mehr erforderlich, wobei dabei freilich stets ein Restrisiko dahingehend verbleibt, ob die jeweilige unternehmerische Darstellung von den Aufsichtsbehörden als hinreichend klar eingeschätzt wird.[99]

[97] Hierzu etwa Mantz, in: Sydow, DS-GVO, 2017, Art. 25 Rn. 57.
[98] Bayerisches Landesamt für Datenschutz, EU-Datenschutz-Grundverordnung, Stand: 04.05.2017, abrufbar unter: https://www.lda.bayern.de/media/baylda_ds-gvo_12_advertising.pdf, jeweils zuletzt abgerufen am 29.05.2017.
[99] Vgl. hierzu weiterführend den demnächst erscheinenden bayme vbm-Leitfaden: Datenschutzrecht 2018 sowie den vbw-Leitfaden: Big Data: Mit Recht!

8 Welche Vorgaben ergeben sich aus dem IT-Sicherheitsrecht?

Pflichten zum Schutz von Vertraulichkeit, Verfügbarkeit und Integrität der Daten

IT-Sicherheit ist gewährleistet, wenn die in einem informationstechnischen System hinterlegten Informationen verfügbar sind, und zwar einschränkend immer dann, wenn dies erforderlich (und vereinbart) ist (*Zugänglichkeit* und *Verfügbarkeit*), für jeden Nutzer, der hierzu berechtigt ist (und dies nachweist), und zwar nur für diesen (*Vertraulichkeit*), mit genau dem Inhalt, den der Urheber geschaffen hat (*Unversehrtheit* und *Integrität*). Zusätzlich müssen die Informationen jedem Urheber in dem Maße zurechenbar sein, in dem der Zweck der Informationsverarbeitung diese Zurechnung fordert (*Zurechenbarkeit* und *Authentizität*).[100] Zusammenfassend beschreibt die IT-Sicherheit damit den Schutz der Vertraulichkeit, Verfügbarkeit und Integrität von elektronisch gespeicherten Informationen vor Bedrohungen technischer Art.[101]

Wie unter Kapitel 5 dargestellt, kann Daten ein enormer wirtschaftlicher Wert innewohnen, sodass Versuche des unberechtigten Zugriffs eine beinahe logische Konsequenz darstellen. Das Feld der möglichen Bedrohungen ist weitreichend und umfasst alles von der gezielten Cyberattacke über Angriffe durch im Internet kursierende Schadprogramme bis hin zum Verlust aufgrund technischer Störungen. Vor allem bei dem Umgang mit teils sensiblen, personenbezogenen Daten ist die Gewährleistung der IT-Sicherheit von höchster Priorität. Nicht zuletzt, um Schadensersatzansprüchen oder anderen Haftungsfolgen zu entgehen, treten zu dem wirtschaftlichen Interesse an der (alleinigen) Verfügungsgewalt über den eigenen Datenbestand auch zwingend einzuhaltende gesetzliche Verpflichtungen zur IT-Sicherheit hinzu.

Regelungen zum IT-Sicherheitsrecht finden sich in mehreren Regelwerken.[102] Dazu gehören das BDSG und die DS-GVO, das Telemediengesetz (TMG), das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) und weitere durch das IT-Sicherheitsgesetz[103] um Regelungen zur IT-Sicherheit ergänzte Gesetze sowie die europäische Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie). Während einige der genannten Regelwerke für jeden Diensteanbieter gelten, gibt es – überwiegend im BSIG – besondere Bestimmungen für Betreiber kritischer Infrastrukturen. Darüber hinaus werden zahlreiche gesetzliche Vorgaben durch zusätzliche Verordnungen des Bundes in rechtlicher, aber vor allem technischer Hinsicht konkretisiert.

---

[100] *Heckmann,* in: Heckmann, jurisPK-Internetrecht, 5. Aufl. 2017, Kap. 5 Rn. 219 m.w.N.
[101] Reinhard, in: Reinhard, IT-Sicherheit und Recht, 2007, Rn. 1.
[102] Vgl. weiterführend zur Thematik den bayme vbm-Leitfaden zur Erstellung von IT-Sicherheitskonzepten: IT-Sicherheit als Rechtspflicht, 2016.
[103] Das IT-Sicherheitsgesetz, Broschüre des Bundesamtes für Sicherheit in der Informationstechnik, S. 5, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/IT-Sicherheitsgesetz.pdf?__blob=publicationFile&v=5, zuletzt abgerufen am 25.05.2017.

8.1 Allgemeine Vorschriften

Im BDSG regelt § 9 BDSG als zentrale Norm den rechtlichen Rahmen der Datensicherheit. Er gibt der verantwortlichen Stelle auf, technische und organisatorische Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Die programmatisch gehaltene Vorschrift wird durch eine zugehörige Anlage präzisiert und ergänzt, sodass § 9 BDSG nur einheitlich mit dieser betrachtet werden kann. Die in dieser Anlage genannten Maßnahmen sind Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags-, Verfügbarkeits- und Datentrennungskontrolle sowie geeignete Verschlüsselungsverfahren. Prägender Gedanke dieser Regelungsinhalte ist dabei das in § 9 Satz 2 BDSG niedergelegte Verhältnismäßigkeitsprinzip, unter dessen Vorbehalt jegliche Umsetzungsmaßnahme steht.[104] Hiernach müssen der Aufwand der Umsetzung der Maßnahme und der angestrebte Schutzzweck in einem angemessenen Verhältnis stehen.[105]

Im hauptsächlich durch das TMG geregelten Online-Bereich ist für die Gewährleistung von IT-Sicherheit insbesondere der mit dem IT-Sicherheitsgesetz neu geschaffene § 13 Abs. 7 TMG von Relevanz. Nach diesem haben Diensteanbieter – unter Berücksichtigung des Stands der Technik und der wirtschaftlichen Zumutbarkeit – durch technische und organisatorische Vorkehrungen sicherzustellen, dass kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist. Außerdem sind Telemedien gegen Verletzungen des Schutzes personenbezogener Daten und Störungen zu sichern. Mit Blick auf das Verhältnis dieser Vorschrift zu den bereits vor deren Einführung geltenden Sicherheitsvorschriften wie § 9 BDSG, d. h. zur Frage, ob etwa beide Vorschriften nebeneinander gelten, herrscht bislang in der juristischen Fachliteratur noch Uneinigkeit.[106]

Das europarechtliche Äquivalent zu § 9 BDSG bzw. § 13 Abs. 7 TMG ist vor allem Art. 32 DS-GVO. In Art. 32 Abs. 1 lit. b DS-GVO finden sich auch die Schutzziele der IT-Sicherheit in Form von Vertraulichkeit, Integrität und Verfügbarkeit wieder. Weiterhin bilden auch nach Art. 32 Abs. 1 DS-GVO der Stand der Technik und die Implementierungskosten die Grenzen der IT-Sicherheit, wodurch auch auf europäischer Ebene dem Verhältnismäßigkeitsgedanken Rechnung getragen wird. Auch im neuen BDSG findet – zumindest in abstrakterer Formulierung – die IT-Sicherheit Erwähnung, zum einen in § 47 Nr. 6 BDSG n.F.:

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet; hierzu gehört auch ein durch geeignete technische und organisatorische Maßnahmen zu gewährleistender Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung."

---

[104] Gola/Klug/Körffer, in: Gola/Schomerus, BDSG, 12. Aufl. 2015, § 9 Rn. 7 f.
[105] Schmidl, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 2016, § 28 Rn. 63.
[106] Karg, in: Wolff/Brink, Beck'scher Online-Kommentar Datenschutzrecht, 19. Edition (Stand: 01.02.2017), § 9 Rn. 31.

Der Anwendungsbereich dieser Norm bezieht sich allerdings nur auf die Verarbeitung personenbezogener Daten durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständigen öffentlichen Stellen (§ 45 BDSG n.F.) und erlangt daher keine allgemeine Geltung. Zum anderen legt § 22 Abs. 2 BDSG n.F. für die besonderen Kategorien personenbezogener Daten Vorgaben fest, die denen des § 9 BDSG a.F. mitsamt seiner Anlage sehr ähnlich sind. Insbesondere erwähnt § 22 Abs. 2 Nr. 7 BDSG n.F. die Verschlüsselung personenbezogener Daten.

8.2 Besondere Vorgaben im Zusammenhang mit kritischen Infrastrukturen

Weiterhin finden sich im BSIG zahlreiche Regelungen zur IT-Sicherheit, darunter vor allem die Festsetzung von Mindeststandards an die IT-Sicherheit und weitergehenden Untersuchungsbefugnissen des Bundesamts für Sicherheit in der Informationstechnik (BSI) sowie die Verpflichtung, erhebliche IT-Störungen an das BSI zu melden (vgl. insbesondere §§ 8a, 8b BSIG).[107] Diese gelten jedoch ausschließlich für Betreiber sog. kritischer Infrastrukturen. Nach § 2 Abs. 10 Satz 1 BSIG sind dies im Wesentlichen Einrichtungen, deren Funktionieren von hoher Bedeutung für das Gemeinwesen und die öffentliche Sicherheit ist. Eine Konkretisierung erfährt das letztgenannte Kriterium durch die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV).[108] Deren erster Teil regelt die Sektoren Energie, Informationstechnik und Telekommunikation, Wasser sowie Ernährung und ist seit dem 03. Mai 2016 in Kraft. Der zweite Teil der Verordnung betrifft die Sektoren Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr. Er ist seit dem 30. Juni 2017 in Kraft.[109] In der BSI-KritisV sind dabei jeweils die Schwellenwerte und Grenzen geregelt, ab deren Überschreiten die entsprechende Anlage als Kritische Infrastruktur gilt.

Beispiele

Nach dem zweiten Teil der BSI-KritisV gelten etwa Güterbahnhöfe ab 23.000 ausgehenden Zügen im Jahr oder Verkehrssteuerungs- und Leitsysteme des ÖPNV ab 125 Millionen Fahrgästen pro Jahr als Kritische Infrastrukturen im Sektor Transport und Verkehr.

[107] Das IT-Sicherheitsgesetz, Broschüre des Bundesamtes für Sicherheit in der Informationstechnik, S. 5, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/IT-Sicherheitsgesetz.pdf?__blob=publicationFile&v=5, zuletzt abgerufen am 25.05.2017.
[108] Abrufbar unter: https://www.gesetze-im-internet.de/bsi-kritisv/index.html#BJNR095800016BJNE000100000, zuletzt abgerufen am 14.11.2017.
[109] BGBl. I 2017, S. 1903.

Auch ohne selbst Betreiber einer kritischen Infrastruktur zu sein, können die Vorgaben des BSIG für bayerische Unternehmen relevant sein. So können etwa gerade Zulieferer und Dienstleister in der Industrie 4.0 wie z. B. Unternehmen, die auch Wartungsaufgaben übernehmen, über die Einkaufsbedingungen ihrer Vertragspartner zur Einhaltung der IT-Sicherheitsvorgaben und ggf. auch deren Nachweis durch Audits oder Zertifizierungen verpflichtet sein.[110] Hintergrund ist, dass die Betreiber Kritischer Infrastrukturen ihren eigenen Anforderungen nur dann ausreichend beikommen können, wenn auch die von ihnen verwendeten Komponenten (nachweislich) sicher sind.[111]

Auf europarechtlicher Ebene werden viele der vorgenannten Vorgaben des BSIG sowie auch des TMG wiederum durch die NIS-Richtlinie überlagert. Mit dieser wurden am 06. Juli 2016 einheitliche europäische Vorgaben zur IT-Sicherheit von Betreibern „wesentlicher Dienste“ (entspricht den Betreibern Kritischer Infrastrukturen im Sinne des BSIG) sowie Anbietern „digitaler Dienste“ (entspricht den Anbietern von Telemediendiensten im Sinne des TMG) beschlossen, darunter etwa Meldepflichten oder der EU-weite Aufbau nationaler Kapazitäten für Cyber-Sicherheit.[112] Der Umsetzungsbedarf in nationales Recht hält sich jedoch angesichts der bereits dargestellten, umfassenden IT-sicherheitsrechtlichen Vorgaben in Grenzen.[113]

Das IT-Sicherheitsrecht ist und bleibt ein wichtiger Faktor beim Umgang mit Daten. Es liegt in der Natur der Sache, dass Investitionen in die Abwehr von IT-Bedrohungen oftmals keine unmittelbar wahrnehmbaren Wirkungen zeigen. Die nachträgliche Folgenbeseitigung im Schadensfall erweist sich in der Regel jedoch als weitaus kostenintensiver als präventive Sicherheitsinvestitionen. Neben technischen Schäden an Anlagen und einem völligen Verlust bzw. zumindest einer erheblichen Beeinträchtigung des Datenbestands können bei Verletzung der relevanten IT-sicherheitsrechtlichen Vorschriften aufsichtsrechtliche Bußgelder und strafrechtliche Folgen sowie Schadensersatzforderungen – auch ggf. von Mitbewerbern[114] – hinzutreten, zudem droht insoweit stets ein ggf. erheblicher Reputationsverlust.[115] Wie schon mit Blick auf den Datenschutz können sich demgegenüber auch hier für Anbieter von sicherheitsrechtlich vorausschauenden, intelligenten Systemen durchaus signifikante Marktvorteile ergeben.[116]

---

[110] Vgl. Hornung/Hofmann, Rechtsfragen bei Industrie 4.0: Rahmenbedingungen, Herausforderungen und Lösungsansätze, in: Reinhart, Handbuch Industrie 4.0, 2017, S. 191, 207 f.
[111] Hornung/Hofmann, Rechtsfragen bei Industrie 4.0: Rahmenbedingungen, Herausforderungen und Lösungsansätze, in: Reinhart, Handbuch Industrie 4.0, 2017, S. 191, 207.
[112] Hierzu etwa: Voigt/Gehrmann, ZD 2016, 355 ff.
[113] Vgl. die Pressemitteilung des Bundesinnenministeriums v. 25.01.2017, abrufbar unter: http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2017/01/nis-umsetzungsgesetz.html, zuletzt abgerufen am 29.05.2017.
[114] Vgl. hierzu etwa Byok, BB 2017, 451, 453 f., der § 8a BSIG als wettbewerbsrechtliche Marktverhaltensregelung i.S.d. § 3a UWG einstuft.
[115] Ausführlich hierzu: Schmidl, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 2016, § 28 Rn. 130 ff.
[116] Vgl. Hornung/Hofmann, Rechtsfragen bei Industrie 4.0: Rahmenbedingungen, Herausforderungen und Lösungsansätze, in: Reinhart, Handbuch Industrie 4.0, 2017, S. 191, 208.

9 Querbeziehungen der unterschiedlichen Regelungsmaterien

Datenschutzrecht, Vertragsrecht und Wettbewerbsrecht

Mit der Darstellung der einzelnen rechtlichen Anknüpfungspunkte ist der Komplexität des Themas „Daten als Wirtschaftsgut“ bei weitem noch nicht Genüge getan. Das grundsätzliche Problem besteht darin, dass auf die entsprechenden Sachverhalte viele einzelne Tatbestände parallel anwendbar sind. Diese sind jedoch oft nicht aufeinander abgestimmt.[117] Im unternehmerischen Kontext muss daher in diesem Zusammenhang häufig eine rechtsgebietsübergreifende und umfassende Gesamtbetrachtung angestellt werden, da nur auf diese Weise die Wechselwirkungen zwischen den einzelnen Rechtsgebieten genau und umfassend erfasst werden können. Leider wird eine derartige umfassende Gesamtbetrachtung in Zeiten der zunehmenden Spezialisierung auf einzelne Rechtsgebiete vonseiten interner Unternehmensjuristen oder auch externer Berater kaum vorgenommen.

Besondere Wechselwirkungen bestehen zwischen dem Datenschutzrecht und dem Vertragsrecht. Hier stellt sich insbesondere die Frage, wie sich datenschutzrechtliche Verstöße auf das Vertragsverhältnis auswirken. Aber auch wettbewerbsrechtliche Verstöße können unter Umständen Auswirkungen auf das Vertragsverhältnis haben. Schließlich kann es zwischen dem Datenschutzrecht und dem Wettbewerbsrecht zu Wechselwirkungen kommen.

9.1 Rechtsgebietsübergreifende Regelungen

Es existieren verschiedene Regelungen, beispielsweise im Vertrags- oder im Wettbewerbsrecht, die rechtsgebietsübergreifende Verbindungen herstellen. Unter 9.2 werden diese – hier zunächst abstrakt zu erläuternden – Vorgaben auf für diesen Leitfaden relevante Rechtsmaterien angewendet.

9.1.1 Vertragsrecht

Für das Vertragsrecht spielt in diesem Zusammenhang zunächst § 134 BGB eine zentrale Rolle:

[117] Heun/Assion, CR 2015, 812, 816.

Ein Rechtsgeschäft, das gegen ein gesetzliches Verbot verstößt, ist nichtig, wenn sich nicht aus dem Gesetz ein anderes ergibt.

Diese Norm gewährleistet damit die Verzahnung zwischen dem Vertragsrecht und anderen Rechtsgebieten. Ein gesetzliches Verbot kann sich unter anderem aus Parlamentsgesetzen oder aus Rechtsverordnungen ergeben.[118] Dabei ist jedoch nicht jedes Gesetz, das ein Rechtsgeschäft beschränkt, als Verbotsgesetz im Sinne des § 134 BGB einzustufen.[119] Vielmehr ist oft durch Auslegung zu ermitteln, ob der Sinn und Zweck des Gesetzes ein Rechtsgeschäft gerade verbieten will oder nicht.[120] So sind Strafgesetze im Zweifel stets als Verbotsgesetze im Sinne des § 134 BGB anzusehen.[121]

Ein Verbotsgesetz muss sich gegen den Inhalt eines Rechtsgeschäftes richten, gegen seine privatrechtliche Wirksamkeit und damit gegen seinen wirtschaftlichen Erfolg.[122] Gelangt die Auslegung dagegen zu dem Ergebnis, dass das Verbot es nicht bezweckt, das Geschäft als solches zu untersagen, sondern dass es sich lediglich gegen die Umstände seines Zustandekommens wendet, wie etwa im Fall des Ladenschlussgesetzes, so handelt es sich um eine Ordnungsvorschrift, nicht um ein Verbotsgesetz.[123] Im Falle eines *zweiseitigen Rechtsgeschäfts,* wie es auch vorliegt, wenn personenbezogene Daten und die Erklärung der datenschutzrechtlichen Einwilligung als Gegenleistung geschuldet sind*,* muss sich das gesetzliche Verbot gegen beide Vertragsparteien oder gegen nur einen der an dem Rechtsgeschäft Beteiligten richten. Im Falle eines nur einseitigen Verstoßes bleibt die Wirksamkeit dagegen in der Regel unberührt.[124]

Beispiel

Ein Verbotsgesetz im Sinne des § 134 BGB ist beispielsweise § 203 Abs. 1 Nr. 1 StGB. In diesem Tatbestand wird der Verstoß gegen die ärztliche Schweigepflicht unter Strafe gestellt. Ist ein Vertrag gerade auf die Übermittlung derartiger geheimhaltungspflichtiger Informationen gerichtet, so führt dieser Verstoß zu einer Nichtigkeit des Vertrags nach § 134 BGB.[125]

[118] Ellenberger, in: Palandt, BGB, 75. Aufl. 2016, § 134 Rn. 2.
[119] Armbrüster, in: MüKo-BGB, 7. Aufl. 2015, § 134 Rn. 41.
[120] Armbrüster, in: MüKo-BGB, 7. Aufl. 2015, § 134 Rn. 41.
[121] Ellenberger, in: Palandt, BGB, 75. Aufl. 2016, § 134 Rn. 24.
[122] BGH, Urt. v. 19.01.1984 - VII ZR 121/83, NJW 1984, 1175, 1175 - Gültiger Werkvertrag bei einseitigem Verstoß gegen Schwarzarbeitsverbot; Vossler in: Gsell/Krüger/Lorenz/Mayer, beck-online.GROSSKOMMENTAR, Stand: 15.05.2017,,§ 134 BGB Rn. 59-62.
[123] Wendtland in: Bamberger/Roth, BeckOK BGB, 40. Edition 2016, Stand: 01.02.2017, § 134 Rn. 13; Armbrüster in: MüKo-BGB, 7. Aufl. 2015, § 134 Rn. 42.
[124] St. Rspr seit: RG, Beschl. v. 17.03.1905 – V 213/03, RGZ 60, 273, 276 ff., vgl. aus der umfangreichen Rechtsprechung etwa: BGH, Urt. v. 25.09.2014 – IX ZR 25/14, NJW 2014, 3568 Tz. 15 - Folgen des Verbots gewerblicher Tätigkeit von Steuerberatern für Forderungsabtretungen; BGH, Urt. v. 23.02.2012 – I ZR 231/10, GRUR 2012, 1050 Tz. 22 - Unzulässige Kooperationsvereinbarung zwischen Zahnärzten und Dentallaborgesellschaft – Dentallaborleistungen; vgl. auch: Specht, Diktat der Technik – Rematerialisierung der Privatautonomie im Informationstechnologischen Umfeld, im Erscheinen.
[125] Vgl. Armbrüster, in: MüKo-BGB, 7. Aufl. 2015, § 134 Rn. 54.

Auch aus § 138 BGB kann sich eine Nichtigkeit des Vertrags ergeben. Hinsichtlich § 138 BGB sind zwei Alternativen zu unterscheiden, die in den zwei Absätzen der Norm getrennt geregelt sind:

(1) Ein Rechtsgeschäft, das gegen die guten Sitten verstößt, ist nichtig.

(2) Nichtig ist insbesondere ein Rechtsgeschäft, durch das jemand unter Ausbeutung der Zwangslage, der Unerfahrenheit, des Mangels an Urteilsvermögen oder der erheblichen Willensschwäche eines anderen sich oder einem Dritten für eine Leistung Vermögensvorteile versprechen oder gewähren lässt, die in einem auffälligen Missverhältnis zu der Leistung stehen.

– Zunächst ist ein Rechtsgeschäft nichtig, das gegen die guten Sitten verstößt (§ 138 Abs. 1 BGB). Dies ist dann der Fall, wenn ein Verstoß gegen das „Anstandsgefühl aller billig und gerecht Denkenden“ vorliegt.[126] Der Begriff der guten Sitten beschreibt damit ein Minimum sittlicher Handlungsweise im Rechtsverkehr.[127] Sittenwidrig ist ein Rechtsgeschäft danach, wenn es nach seinem Charakter mit den grundlegenden Wertungen der Rechts- und Sittenordnung nicht zu vereinbaren ist. Dies ergibt sich aus Inhalt, Beweggrund und Zweck des Rechtsgeschäfts.[128]

Beispiel

Sittenwidrig sind beispielsweise sog. „Knebelungsverträge“. Durch diese wird durch das Rechtsgeschäft eine derart weitgehende Beschränkung der wirtschaftlichen Freiheit des anderen Vertragspartners bewirkt, dass dieser seine freie Selbstbestimmung ganz oder zumindest im Wesentlichen einbüßt.[129] Dies ist beispielsweise dann der Fall, wenn ein Autor durch seinen Verlag ohne eine entsprechende Gegenleistung dazu verpflichtet wird, dem Verlag alle seine künftigen Werke anzubieten.[130]

– Auch Verträge, die als Hauptleistungspflicht eine strafbare Handlung beinhalten, sind grundsätzlich nach § 138 Abs. 1 BGB sittenwidrig. Sofern jedoch zugleich ein

[126] Ellenberger, in: Palandt, BGB, 75. Aufl. 2016, § 138 Rn. 2.
[127] Motive zu dem Entwurfe eines Bürgerlichen Gesetzbuches für das Deutsche Reich, Band II, Recht der Schuldverhältnisse, 1896, S. 727; BGH, Urt. v. 19.07.2004 - II ZR 217/03, NJW 2004, 2668, 2670; BGH, Urt. v. 18.12.2008 - VII ZR 201/06, NJW 2009, 835; st. Rspr seit: RG, Urt. v. 11.04.1901, RGZ 48, 114, 124; vgl. auch: Specht, Diktat der Technik – Rematerialisierung der Privatautonomie im Informationstechnologischen Umfeld, im Erscheinen.
[128] BGH, Urt. v. 03.04.2008 – III ZR 90/07, NJW 2008, 2026, Tz. 21 ff. - Online-Roulette; Wendtland in: Bamberger/Roth, BeckOK BGB, 40. Edition 2016, Stand: 01.02.2017, § 138 Rn. 19; Arnold in: Erman, BGB, 14. Aufl. 2014, § 138 Rn. 14; Mansel in: Jauernig, BGB, 16. Aufl. 2015, § 138 Rn. 8; Ahrens in: Prütting/Wegen/Weinreich, BGB, 10. Aufl. 2015, § 138 Rn. 24; vgl. auch: Specht, Diktat der Technik – Rematerialisierung der Privatautonomie im Informationstechnologischen Umfeld, im Erscheinen.
[129] Ellenberger, in: Palandt, BGB, 75. Aufl. 2016, § 138 Rn. 39.
[130] Armbrüster, in: MüKo-BGB, 7. Aufl. 2015, § 138 Rn. 71.

Verstoß gegen ein Verbotsgesetz vorliegt, ist in diesem Fall § 134 BGB die vorrangig anzuwendende Norm.[131] Keinesfalls ist der Einsatz von Daten – auch soweit diese einen Personenbezug aufweisen – *per se* als sittenwidrig anzusehen.

– In § 138 Abs. 2 BGB ist der sog. Wucher-Tatbestand geregelt. Nach diesem ist ein Rechtsgeschäft nichtig, durch das jemand unter Ausbeutung der Zwangslage, der Unerfahrenheit, des Mangels an Urteilsvermögen oder der erheblichen Willensschwäche eines anderen sich oder einem Dritten für eine Leistung Vermögensvorteile versprechen oder gewähren lässt, die in einem auffälligen Missverhältnis zu der Leistung stehen. Ein auffälliges Missverhältnis zwischen Leistung und Gegenleistung liegt dann vor, wenn die Leistung, die vom Schuldner erbracht werden muss, zu 100 Prozent oder mehr über dem Marktpreis liegt (sog. „Grenze des Doppelten“).[132]

Beispiel

Bei einer Telefonrechnung über knapp 7.600 EUR für den Download von 844 MB Datenvolumen eines Verbrauchers (ohne Datentarif) könnte mit guten Gründen ein „Datenwucher“ angenommen werden.[133] Einen weiteren denkbaren Anwendungsfall könnte – bezogen auf den B2B-Verkehr – etwa auch das Angebot einer Unternehmensberatung bilden, welche sich für ein einfaches Auswertungstool von dem Vertragspartner den gesamten vorhandenen Datenbestand übermitteln lässt. Beispiele aus der Rechtsprechung fehlen hierzu jedoch bislang leider vollständig.

– Ferner erfordert § 138 Abs. 2 BGB ein auffälliges Missverhältnis zwischen Leistung und Gegenleistung und infolgedessen einen auf einen Leistungsaustausch gerichteten Vertrag. Damit setzt die Anwendung dieser Vorschrift wiederum voraus, dass Daten als Vertragsgegenstand eingeordnet werden. Allerdings stellt sich auch hier das Problem der Bestimmung des Werts der Daten, da nur so das Vorliegen eines auffälligen Missverhältnisses bejaht werden kann (siehe hierzu unter 5.). Hinzu kommt, dass es zur Bestimmung des auffälligen Missverhältnisses auf den Zeitpunkt des Vertragsschlusses ankommt. Ein nachträglich entstehendes Missverhältnis ist dagegen von § 138 Abs. 2 BGB grundsätzlich nicht erfasst.[134] Der Wert der Daten wird jedoch gerade auch durch die nachträgliche Verknüpfung mit anderen Daten bestimmt.

[131] Ellenberger, in: Palandt, BGB, 75. Aufl. 2016, § 138 Rn. 13.
[132] Ellenberger, in: Palandt, BGB, 75. Aufl. 2016, § 138 Rn. 67.
[133] Vgl. law blog-Eintrag v. 22.09.2009, https://www.lawblog.de/index.php/archives/2009/09/22/was-durfen-844-mb-daten-kosten/, zuletzt abgerufen am 14.06.2017. Die Forderung wurde vom betreffenden Anbieter jedoch niedergeschlagen.
[134] Ellenberger, in: Palandt, BGB, 75. Aufl. 2016, § 138 Rn. 66.

– Diese Ausführungen zeigen, dass die Anwendung des § 138 Abs. 2 BGB für die Verwendung von Daten als Gegenleistung zu erheblichen Schwierigkeiten führen kann, was durchaus einige Schutzlücken auf Seiten des Datenschuldners offenbart.

9.1.2 Wettbewerbsrecht

Die Verknüpfung der verschiedenen Rechtsgebiete mit dem Wettbewerbsrecht erfolgt unter anderem durch § 3a UWG, der eine Regelung über den Begriff der unlauteren Handlung enthält:

Unlauter handelt, wer einer gesetzlichen Vorschrift zuwiderhandelt, die auch dazu bestimmt ist, im Interesse der Marktteilnehmer das Marktverhalten zu regeln, und der Verstoß geeignet ist, die Interessen von Verbrauchern, sonstigen Marktteilnehmern oder Mitbewerbern spürbar zu beeinträchtigen.

Diese gesetzlichen Vorschriften werden auch als Marktverhaltensregelungen bezeichnet.[135] Unter den Begriff der gesetzlichen Vorschrift fällt jede Rechtsnorm, die in der Bundesrepublik Deutschland Geltung beansprucht, also beispielsweise Gesetze, Rechtsverordnungen oder Rechtsvorschriften der Europäischen Union, soweit diese in den Mitgliedstaaten unmittelbar verbindlich sind (z. B. EU-Verordnungen).[136]

Unlautere Handlungen sind wettbewerbsrechtlich unzulässig (§ 3 Abs. 1 UWG) und können im Rahmen des Wettbewerbsrechts selbst zu einem Anspruch auf Beseitigung oder Unterlassung (§ 8 Abs. 1 UWG) oder auch zu einem Anspruch auf Schadensersatz führen (§ 9 Satz 1 UWG).

9.2 Anwendung der rechtsgebietsübergreifenden Regelungen auf relevante Rechtsmaterien

9.2.1 Querbeziehung zwischen Vertragsrecht und Datenschutzrecht

Ob ein Verstoß gegen Datenschutzvorschriften zu einer Nichtigkeit des Vertrags im Sinne des § 134 BGB führt, hängt von der Einordnung der datenschutzrechtlichen Vorschriften als Verbotsgesetze ab. Diese Frage ist bisher noch nicht umfassend geklärt.[137] Mit Blick auf den Zweck des Datenschutzrechts kann die Ansicht vertreten

---

[135] Vgl. v. Jagow in: Harte-Bavendamm/Henning-Bodewig, UWG, 4. Aufl. 2016, § 3a Rn. 22.
[136] V. Jagow, in: Harte-Bavendamm/Henning-Bodewig, UWG, 4. Aufl. 2016, § 3a Rn. 13; Köhler, in: Köhler/Bornkamm, UWG, 35. Aufl. 2017, § 3a Rn. 1.52.
[137] Für eine umfassende Charakterisierung der datenschutzrechtlichen Normen als Verbotsgesetze vgl. aber: Specht, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung – Die zivilrechtliche Erfassung des Datenhandels, 2012.

werden, dass auch die datenschutzrechtlichen Vorschriften, wie etwa das in § 4 Abs. 1 BDSG bzw. Art. 6 Abs. 1 DS-GVO geregelte Verbot mit Erlaubnisvorbehalt, Verbotsgesetze im Sinne des § 134 BGB darstellen.[138]

Der Zweck des Datenschutzrechts besteht darin, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird (§ 1 Abs. 1 BDSG bzw. Art. 1 DS-GVO). Das Datenschutzrecht gilt im persönlichen Bereich für jede einzelne Person und ist daher für jedermann von enormer Bedeutung. Hinter dem umfassenden Schutz der Daten steht die grundrechtliche Gewährleistung des Rechts auf informationelle Selbstbestimmung. Zentrales Merkmal des nationalen Datenschutzrechts ist das sog. Verbot mit Erlaubnisvorbehalt. Dieser in § 4 Abs. 1 BDSG niedergelegte Grundsatz, dass eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten nur dann zulässig ist, soweit ein gesetzlicher Erlaubnistatbestand vorliegt oder der Betroffene eingewilligt hat, zeigt den enormen Schutzbedarf dieser personenbezogenen Daten. Eine diesem Grundsatz vergleichbare Regelung findet sich auch in Art. 6 Abs. 1 DS-GVO. Es erscheint daher nachvollziehbar, dies als Verbotsgesetz im Sinne des § 134 BGB einzuordnen.

Ob dieses Ergebnis auf alle Regelungen des BDSG bzw. der DS-GVO übertragen werden kann, ist jedoch zweifelhaft, da die jeweiligen Vorgaben unterschiedliche Zielrichtungen verfolgen. Während § 4 Abs. 1 BDSG bzw. Art. 6 Abs. 1 DS-GVO die Zulässigkeit der Datenverarbeitung betrifft (d.h. das „Ob“ der Datenverarbeitung), betrifft beispielsweise die Regelung der Datenvermeidung und Datensparsamkeit bzw. Datenminimierung (§ 3a BDSG bzw. Art. 5 Abs. 1 lit. c DS-GVO) die Art und Weise der Datenverarbeitung (d.h. das „Wie“ der Datenverarbeitung). Ob ein Verstoß gegen letztere Vorgaben dabei bereits in jedem Fall zur Nichtigkeit des Vertrags führen soll, erscheint somit sehr fraglich.

Doch selbst wenn das Vorliegen eines Verbotsgesetzes nach § 134 BGB verneint wird, kann auch im Bereich der datenschutzrechtlichen Vorschriften ein Rechtsgeschäft sittenwidrig und daher nach § 138 Abs. 1 BGB nichtig sein. § 138 Abs. 1 BGB schützt insbesondere auch die Wertentscheidungen des Grundgesetzes und die dahinterstehenden Rechte des Einzelnen.[139] Die Generalklausel des § 138 Abs. 1 BGB wird als „Einfallstor“ der Grundrechte in das Privatrecht bezeichnet.[140] Bedeutet die Verpflichtung eines Rechtsgeschäfts zugleich die Verletzung des Rechts auf informationelle Selbstbestimmung, so führt dies zur Nichtigkeit des Vertrags nach § 138 Abs. 1 BGB.

[138] Siehe hierzu ebenso Specht, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung: Die zivilrechtliche Erfassung des Datenhandels, 2012, Kap. 10 Rn. 561.
[139] Ellenberger, in: Palandt, BGB, 75. Aufl. 2016, § 138 Rn. 42.
[140] Vgl. Armbrüster, in: MüKo-BGB, 7. Aufl. 2015, § 138 Rn. 20.

Beispiel

Ein Vertrag, der es dem Unternehmer gestattet, die personenbezogenen Daten von Kunden des anderen Vertragspartners ohne deren Einwilligung zu verarbeiten, verstößt aufgrund des Fehlens einer gesetzlichen Ermächtigungsgrundlage gegen das Verbot mit Erlaubnisvorbehalt aus § 4 Abs. 1 BDSG bzw. Art. 6 Abs. 1 DS-GVO und ist nach der hier vertretenen Auffassung nach § 134 BGB nichtig. Wird ein Verstoß gegen ein Verbotsgesetz verneint, so ist der Vertrag jedenfalls sittenwidrig und nach § 138 Abs. 1 BGB nichtig, was damit zum selben rechtlichen Ergebnis führt. Aufgrund der Nichtigkeit des Vertrags kommen grundsätzlich bereicherungsrechtliche Rückabwicklungsansprüche nach den §§ 812 ff. BGB, insbesondere eine Leistungskondiktion nach § 812 Abs. 1 Satz 1 Alt. 1 BGB, in Betracht. In der Folge ist somit das jeweils Geleistete (abhängig vom Vertragsinhalt) zurückzugewähren. Ist eine Herausgabe des Erlangten wegen seiner Beschaffenheit nicht möglich – was bei Daten häufig der Fall sein wird – so besteht der Bereicherungsanspruch in einem Anspruch auf Wertersatz, gem. § 818 Abs. 2 BGB. Der Anspruch des Unternehmers kann jedoch in diesen Fällen aufgrund des Verstoßes gegen § 134 BGB oder zumindest § 138 Abs. 1 BGB nach § 817 Satz 2 BGB analog ausgeschlossen sein.

9.2.2 Querbeziehung zwischen Vertragsrecht und Wettbewerbsrecht

Mit Blick auf die Querbeziehung zwischen Vertrags- und Wettbewerbsrecht ist wiederum § 134 BGB als maßgebliche Vorschrift zu nennen. Hinsichtlich der Einordnung der Regelungen des UWG als Verbotsgesetze ist grundsätzlich zwischen zwei Fallkonstellationen zu unterscheiden:

– Verträge die gerade aufgrund eines Wettbewerbsverstoßes zustande gekommen sind (sog. Folgeverträge), sind vertragsrechtlich grundsätzlich wirksam.[141] Der Grund besteht darin, dass das UWG nur Regelungen über die Art des Zustandekommens, aber nicht über den Inhalt des Rechtsgeschäfts trifft.[142]

Beispiel

In § 16 Abs. 1 UWG ist das Verbot der irreführenden Werbung geregelt. Wird ein Vertrag aufgrund der irreführenden Werbung geschlossen, so ist dieser wirksam, da sich

[141] Armbrüster, in: MüKo-BGB, 7. Aufl. 2015, § 134 Rn. 67.
[142] Ellenberger, in: Palandt, BGB, 75. Aufl. 2016, § 134 Rn. 24.

das Verbot gerade nicht gegen den Inhalt des Folgevertrags richtet. Dabei können beispielsweise nicht zutreffende Werbeaussagen über die materielle Rechtmäßigkeit der Datenverarbeitung, über den Einsatz von technisch-organisatorischen Maßnahmen oder über die datenschutzrechtliche Zuverlässigkeit von am Verfahren beteiligten Stellen irreführend sein.[143] Für den getäuschten Vertragspartner besteht in diesen Fällen jedoch die Möglichkeit der Anfechtung des Vertrags nach § 123 Abs. 1 BGB wegen arglistiger Täuschung.[144]Zu beachten ist ferner, dass die Durchsetzung der Erfüllung derartiger Verträge wiederum einen Wettbewerbsverstoß im Sinne des § 3 UWG darstellen kann, wodurch Mitbewerber wiederum auf eine Untersagung hinwirken können.[145]

– Auf europäischer Ebene gibt es Tendenzen, die diese Systematik grundlegend ändern können. Es wird aktuell ein Individualrechtsbehelf bei Verstößen gegen das Wettbewerbsrecht angestrebt[146], und die zunehmend verbraucherschützende Ausrichtung des europäischen Lauterkeitsrechts macht es zugleich wahrscheinlicher, dass auch deutsche Gerichte hier von einer Nichtigkeit ausgehen. So hat zuletzt mindestens ein erstinstanzliches Gericht die Nichtigkeit des (Folge-)Vertrags nach § 134 BGB wegen des Verstoßes gegen das UWG angenommen (AG Bremen, Urteil vom 21. November 2013, Az. 9 C 573/12 zu sog. Cold Calls, d. h. unerlaubter Telefonwerbung).

– Schon heute gilt: Beinhaltet gerade die vertragliche Verpflichtung selbst ein wettbewerbswidriges Verhalten, so fungieren die Regelungen des UWG als Verbotsgesetze im Sinne des § 134 BGB.[147] Der Vertrag ist somit nach § 134 BGB nichtig.

Beispiel

Beinhaltet ein Rechtsgeschäft die Verpflichtung zur verbotswidrigen und strafbaren Offenbarung von Betriebs- und Geschäftsgeheimnissen wie z. B. die Weitergabe von geheimen Daten aus Anlagen im Betrieb eines Dritten (§ 17 UWG), so ist der dieser Verpflichtung zugrundeliegende Vertrag nach § 134 BGB nichtig, da gerade die vertragliche Verpflichtung selbst ein wettbewerbswidriges Verhalten verlangt.[148]

---

[143] Weichert, VuR 2006, 377, 380.
[144] Vossler, in: Gsell/Krüger/Lorenz/Mayer, beck-online.GROSSKOMMENTAR, Stand: 15.05.2017, § 134 BGB Rn. 248.
[145] Vossler, in: Gsell/Krüger/Lorenz/Mayer, beck-online.GROSSKOMMENTAR, Stand: 15.05.2017, § 134 BGB Rn. 246.1.
[146] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richt-linie 93/13/EWG des Rates vom 5. April 1993 (missbräuchliche Vertragsklauseln), der Richtlinie 98/6/EG des Europäischen Parlaments und des Rates (Preisangaben), der Richtlinie 2005/29/EG des Europäischen Parlaments und des Rates (unlautere Geschäftspraktiken) sowie der Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates (Verbraucherrechterichtlinie) zur besseren Durchsetzung und Modernisierung der EU-Verbraucherschutzvorschriften COM(2018) 185 final
[147] Ellenberger, in: Palandt, BGB, 75. Aufl. 2016, § 134 Rn. 24; Armbrüster, in: MüKo-BGB, 7. Aufl. 2015, § 134 Rn. 67.
[148] Vossler, in: Gsell/Krüger/Lorenz/Mayer, beck-online.GROSSKOMMENTAR, Stand: 15.05.2017, § 134 BGB Rn. 249.

Liegt eine Nichtigkeit nach § 134 BGB nicht vor, so kommt noch immer eine Nichtigkeit nach § 138 Abs. 1 BGB in Betracht. Da der Zweck des UWG darin besteht, neben den Mitbewerbern auch Verbraucherinnen und Verbraucher sowie sonstige Marktteilnehmer vor unlauteren geschäftlichen Handlungen zu schützen (§ 1 Satz 1 UWG), wird argumentiert, dass die Verletzungen der Regelungen des UWG zu einer Nichtigkeit des Vertrags wegen Sittenwidrigkeit führen sollen.[149]

9.2.3 Querbeziehung zwischen Datenschutzrecht und Wettbewerbsrecht

Können auch Datenschutzverstöße wettbewerbsrechtlich geahndet werden? Dies wird aufgrund der besonderen Bedeutung der Daten für ökonomische Zwecke und der daraus folgenden Einordnung der Daten als Wirtschaftsgut größtenteils befürwortet. Insbesondere wird argumentiert, dass den Daten neben dem Schutz über das Recht auf informationelle Selbstbestimmung auch ein wettbewerblicher Marktbezug zuerkannt werden müsse, zumal den Daten neben dem ideellen Wert auch eine vermögensrechtliche Qualität zukomme (vgl. unter 4.).[150]

In der Rechtsprechung wird diese Frage dagegen uneinheitlich beantwortet.[151] Handelt ein Unternehmen im Rahmen eines Wettbewerbsverhältnisses entgegen datenschutzrechtlicher Bestimmungen, indem es beispielsweise Daten ohne gesetzlichen Erlaubnistatbestand und ohne eine Einwilligung des Betroffenen verarbeitet (vgl. § 4 Abs. 1 BDSG), so ist umstritten, ob ein derartiger Verstoß als unlautere Handlung im Sinne des § 3a UWG eingestuft werden kann.

Da Verstöße gegen das Datenschutzrecht dem Unternehmer auch einen Wettbewerbsvorteil verschaffen können, wird man insbesondere in diesem Fall von einer unlauteren Handlung ausgehen müssen.[152] Eine derartige unlautere Handlung ist unzulässig (§ 3 Abs. 1 UWG) und führt grundsätzlich zu einem Beseitigungs- oder Unterlassungsanspruch (§ 8 Abs. 1 UWG), der von Mitbewerbern, Einrichtungen zum Schutz der Verbraucherinteressen und anderen rechtsfähigen Verbänden und qualifizierten Einrichtungen im Sinne des § 8 Abs. 3 UWG geltend gemacht werden kann. Bei Entstehen eines Schadens ist derjenige, der die unzulässige Handlung vornimmt, den Mitbewerbern zum Ersatz des Schadens verpflichtet (§ 9 Satz 1 UWG).[153] Ein Mitbewerber ist jeder Unternehmer, der mit einem oder mehreren Unternehmern als Anbieter oder Nachfrager von Waren oder Dienstleistungen in einem konkreten Wettbewerbsverhältnis steht (§ 2 Abs. 1 Nr. 3 UWG).

---

[149] Armbrüster, in: MüKo-BGB, 7. Aufl. 2015, § 138 Rn. 8.
[150] Galetzka, K&R 2015, 77.
[151] Dafür: OLG Köln, Urt. v. 19.11.2010 – 6 U 73/10; dagegen: OLG München, Urt. v. 12.01.2012 – 29 U 3926/11.
[152] Vgl. hierzu Kraska, Der Datenschutz: als Marktverhaltensregel, abrufbar unter: http://www.it-recht-kanzlei.de/datenschutz-marktverhaltensregel.html?print=1, zuletzt abgerufen am 21.06.2017.
[153] Vgl. hierzu Bäcker in: Wolff/Brink, Beck-OK Datenschutzrecht, 19. Edition, Stand: 01.02.2017, § 4 BDSG Rn. 23.

9.3 Fazit und Auswirkungen für bayerische Unternehmen

Die vorstehenden Ausführungen zeigen, wie komplex Fallgestaltungen sein können, in denen die Regelungen mehrerer Rechtsgebiete parallel anwendbar sind. Es ist schwer zu bestimmen, welche Verstöße sich in welcher Weise auf die Regelungsmaterien der anderen Rechtsgebiete auswirken. Daher ist es von zentraler Bedeutung, diese einzelnen Regelungen nicht gesondert, sondern im Wege einer umfassenden Gesamtbetrachtung zu erfassen. (Nicht nur) Unternehmen ist daher zu empfehlen, in rechtlichen Angelegenheiten darauf zu achten, dass sämtliche in Betracht kommende Regelungsbereiche bei der rechtlichen Würdigung berücksichtigt werden. Nur so können unliebsame und unter Umständen auch dem Unternehmen schadende Forderungen anderer, wie z. B. von Mitbewerbern, vermieden werden.

10 Zusammenfassung und Ausblick

Anregungen zum weiteren Vorgehen

1. Für den Begriff der „Daten“ hat sich bislang noch keine rechtsgebietsübergreifende Definition durchgesetzt. Der begrifflichen Abgrenzung kommt jedoch teilweise eine besonders hohe Bedeutung zu – etwa dann, wenn es um die Anwendbarkeit entsprechender Rechtsbereiche geht. Beispielhaft ist das Datenschutzrecht nur dann anwendbar, soweit es sich um personenbezogene Daten handelt. Demgegenüber bedarf es beim Umgang mit reinen Sachdaten nicht der Beachtung datenschutzrechtlicher Vorgaben.

2. Mit Blick auf das Zivilrecht können Daten in dreierlei Hinsicht eine Rolle spielen: Erstens können sie rein der Vertragserfüllung dienen, zweitens können sie die Gegenleistung eines Vertrages als solcher darstellen und drittens können Daten auch den Gegenstand bestimmter Dienstleistungen – wie etwa Big Data-Analysen oder Cloud Services – bilden.

3. Verbunden mit dem zunehmenden wirtschaftlichen Wert von Daten – wenngleich auch die Bestimmung einer konkreten Höhe besondere Schwierigkeiten aufweist – erlangt die Frage, wer auf sie in rechtmäßiger Weise zugreifen darf, immer mehr an Bedeutung. In der rechtswissenschaftlichen Literatur wird derzeit die Frage nach dem Bestehen eines „Dateneigentums“ vielfach diskutiert. Bejaht man ein solches, steht dem „Dateneigentümer“ aufgrund der mit seiner Stellung verbundenen, umfangreichen Verfügungs- und Abwehrrechte auch das Recht zu, auf die Daten zugreifen und mit ihnen grundsätzlich nach seinem Belieben verfahren zu können. Jedoch sieht zumindest das derzeit geltende Recht mit guten Gründen ausschließlich ein Eigentum an *körperlichen* Sachen vor. Ob dies in Zukunft geändert werden soll, ist auch bereits Gegenstand einer kontrovers geführten (rechts-)politischen Diskussion, dies sowohl auf nationaler als auch europäischer Ebene. Die besseren Argumente sprechen dagegen.

4. Schon auf Basis des derzeit geltenden Rechts bestehen jedoch bestimmte Zugriffs- und Nutzungsbeschränkungen, die sich – neben möglichen vertraglichen Vereinbarungen – insbesondere aus dem Straf-, Wettbewerbs- und Datenschutzrecht ergeben. Beispielsweise können durch die besonders relevanten Vorgaben des wettbewerbsrechtlichen Geheimnisschutzes unbefugte Datenübermittlungen strafbar sein, soweit sie geschützte Geschäfts- und Betriebsgeheimnisse betreffen. Hieraus ergibt sich im Gegenzug eine Zugriffs- und Nutzungsbeschränkung für Dritte.

5. Dass Daten die Gegenleistung eines Vertrages bilden können, sieht ein europarechtlicher Richtlinien-Entwurf explizit vor – jedenfalls, soweit es sich um Daten von Verbrauchern handelt. Dem deutschen Recht liegt der Grundsatz der Vertragsfreiheit zugrunde, welcher den Vertragsparteien erlaubt, den Vertragsgegenstand

grundsätzlich frei zu bestimmen. Welcher Vertragstyp (Tauschvertrag, doppelter Typus etc.) dabei jedoch genau einschlägig ist, beurteilt sich nach dem Inhalt des konkreten Rechts. Auch an anderen Stellen zeigt sich, dass das deutsche Zivilrecht derzeit noch nicht auf Daten als Gegenleistung zugeschnitten ist. Beispielhaft müssen nach deutschem Zivilrecht die wesentlichen Inhalte eines Vertrages bestimmt sein – wie konkret die Bezeichnung der Daten mitsamt des geplanten Verwendungszwecks ausfallen muss, wenn mit Daten „bezahlt" wird, wurde bislang weder durch den Gesetzgeber noch die Rechtsprechung näher konkretisiert. Ganz besonders deutlich zeigt sich dieses Problem bei Big Data-Anwendungen, bei denen im Zeitpunkt des Vertragsschlusses der Verwendungszweck dem Vertragspartner häufig noch nicht einmal im Ansatz bekannt ist.

6. Auch datenschutzrechtliche Vorgaben können den rechtmäßigen Umgang mit Daten beschränken bzw. sogar vollständig ausschließen. Nach dem datenschutzrechtlichen Grundsatz des Verbots mit Erlaubnisvorbehalt bedarf es bei jeder datenschutzrechtlich relevanten Handlung entweder einer gesetzlichen Erlaubnisnorm oder der Einwilligung des Betroffenen. Mangels entsprechend einschlägiger Erlaubnistatbestände ist für den Datenverwender die Einholung der entsprechenden Einwilligungen häufig unumgänglich. An die Einholung einer wirksamen Einwilligung sind jedoch wiederum zahlreiche Voraussetzungen geknüpft – sie muss z. B. informiert sein. Durch den steigenden Wert von Daten gerade erst durch deren Verknüpfung stellen sich hierbei jedoch häufig besondere Herausforderungen.

7. Nicht außer Acht gelassen werden darf auch das IT-Sicherheitsrecht, speziell im Rahmen von Datenverarbeitungen der Betreiber kritischer Infrastrukturen bzw. deren Zulieferer und Dienstleister. Dies betrifft die Sektoren Energie, Informationstechnik und Telekommunikation, Wasser, Ernährung, Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr. Die hiernach Verpflichteten haben dabei etwa geeignete technische und organisatorische Maßnahmen zu ergreifen, um personenbezogene Daten vor unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust oder unbeabsichtigter Schädigung zu schützen.

8. Das Thema „Daten als Wirtschaftsgut" kann schließlich nicht isoliert im Rahmen der einzelnen Rechtsgebiete beleuchtet werden. Denn es bestehen zahlreiche Wechselwirkungen zwischen den einzelnen Regelungsmaterien, die es im Rahmen einer umfassenden Gesamtbetrachtung zu berücksichtigen gilt. Beispielhaft stellt nicht jeder Verstoß gegen datenschutzrechtliche Vorgaben zugleich einen Vertragsverstoß dar, selbst wenn Daten die Gegenleistung des jeweiligen Vertrages bilden. Vielmehr bedarf es hierbei einer Differenzierung zwischen elementaren Vorschriften über die Zulässigkeit der Datenverarbeitung und flankierenden Regelungen im Datenschutzrecht, die teilweise auch nur bloße Programmsätze beinhalten. Beispielhaft erwähnt sei hierbei die generelle Verpflichtung, so wenig Daten als möglich zu erheben.

Wie im Rahmen der einzelnen Themenfelder bereits aufgezeigt, befinden sich derzeit zahlreiche Fragen rund um Daten als Wirtschaftsgut in der rechtspolitischen Diskussion. Diese findet zum einen auf nationaler Ebene – wie etwa mit Blick auf eine grundlegende Reform des Vertragsrechts,[154] insbesondere zur Schaffung eines Dateneigentums (siehe hierzu gesondert unter 4.2) – statt. Neben Letzterem steht zum anderen auch auf europäischer Ebene insbesondere das Thema „Daten als Währung“ auf der politischen Agenda (siehe im Einzelnen hierzu unter 6.2.).[155]

Bayerische Unternehmen sollten die dargestellten Gesetzgebungsvorhaben im Blick behalten und sich bestenfalls schon während der Entwicklung und Implementierung neuer Wertschöpfungsprozesse betreffend den Einsatz von Daten als Wirtschaftsgut, beispielsweise im Rahmen der Datenauswertung oder zur Optimierung von Logistikprozessen – auch und vor allem in der Industrie 4.0 –, hinreichend über rechtliche Anforderungen von fachkundiger Seite beraten lassen, wodurch sich auch die Chance auf Wettbewerbsvorteile sichern lässt.[156]

[154] Vgl. hierzu etwa Stöhr, ZIP 2016, 1468, 1473 f.
[155] Vgl. https://www.golem.de/news/eu-ministerrat-anbieter-sollen-fuer-gratis-apps-haften-1706-128311.html, zuletzt abgerufen am 13.06.2017.
[156] In dieselbe Richtung Hornung/Hofmann, Rechtsfragen bei Industrie 4.0: Rahmenbedingungen, Herausforderungen und Lösungsansätze, in: Reinhart, Handbuch Industrie 4.0, 2017, S. 191, 208.

Ansprechpartner / Impressum

Christine Völzow
Geschäftsführerin
Leiterin der Abteilung Wirtschaftspolitik

Telefon 089-551 78-251
Telefax 089-551 78-249
christine.voelzow@vbw-bayern.de

Impressum

Alle Angaben dieser Publikation beziehen sich grundsätzlich sowohl auf die weibliche als auch auf die männliche Form. Zur besseren Lesbarkeit wurde meist auf die zusätzliche Bezeichnung in weiblicher Form verzichtet.

Herausgeber

bayme
Bayerischer Unternehmensverband Metall und Elektro e. V.

vbm
Verband der Bayerischen Metall- und Elektro-Industrie e. V.

vbw
Vereinigung der Bayerischen Wirtschaft e. V.

Max-Joseph-Straße 5
80333 München

www.baymevbm.de www.vbw-bayern.de

Weiterer Beteiligter

Prof. Dirk Heckmann
Universität Passau

0851-509-2290
heckmann@mein-jura.de

unter Mitwirkung von
Prof. Louisa Specht
Universität Bonn