Datennutzung für digitale Geschäftsmodelle

Leitfaden zu Rechtsfragen und Vertragsgestaltung
Teil 1 – Gesetzliche Grundlagen

www.bitkom.org

bitkom

Herausgeber

Bitkom e. V.
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
Albrechtstraße 10 | 10117 Berlin

Ansprechpartner

Thomas Kriesel | Bitkom e. V.
T 030 27576-146 | t.kriesel@bitkom.org

Verantwortliche Bitkom-Gremien

AK Vertrags- und Rechtsgestaltung

Satz & Layout

Sabrina Fleming | Bitkom e. V.

Titelbild

© michal parzuchowski | unsplash.com

Vorwort und Danksagung

Dieser Leitfaden zur Datennutzung für digitale Geschäftsmodelle ist eine Publikation des Bitkom-Arbeitskreises Vertrags- und Rechtsgestaltung. Der Arbeitskreis besteht aus Rechtsexperten der Bitkom-Mitgliedsunternehmen und befasst sich mit der Vertragsgestaltung in der Digitalbranche und mit den hierfür geltenden gesetzlichen Anforderungen.

Der vorliegende erste Teil des Leitfadens gibt einen Überblick über die gesetzlichen Grundlagen für Austausch und Nutzung von Daten. Darauf aufbauend werden im zweiten Teil des Leitfadens Überlegungen zur Gestaltung von Verträgen über Datenzugang, Datenaustausch und Datennutzung angestellt. Dabei beschränkt sich die Darstellung jedoch auf Vertragsbeziehungen zwischen Unternehmen (B2B). Rechtliche Anforderungen für Vertragsbeziehungen über den Austausch von Daten zwischen Verbrauchern und Unternehmen (B2C) und zwischen der öffentlichen Hand und Unternehmen (B2G) werden nicht betrachtet. Die Untersuchung dieser für Digitalunternehmen ebenfalls sehr relevanten Bereiche bleibt anderen Bitkom-Publikationen vorbehalten.[1]

Der Leitfaden soll Denkanstöße setzen und eine erste Orientierung zu den gesetzlichen und vertraglichen Grundlagen der Datennutzung geben. Er kann aber weder endgültige und umfassende Lösungen präsentieren noch eine Beratung durch externe oder interne Juristen für den konkreten Anwendungsfall ersetzen.

Wir laden alle Interessierten herzlich ein, sich an der Weiterentwicklung des Dokuments zu beteiligen. Ihr Feedback nehmen wir gern entgegen! Für Beiträge, aber auch für Fragen und kritische Anmerkungen steht Ihnen der Arbeitskreis Vertrags- und Rechtsgestaltung im Bitkom gern zur Verfügung. Bitte senden Sie Ihre Rückmeldungen per Mail an ↗t.kriesel@bitkom.org.

Diese Publikation beruht auf der spezifischen Sachkenntnis, der wertvollen praktischen Erfahrung und auf dem ehrenamtlichen Engagement von Experten aus den Bitkom-Mitgliedsunternehmen. Für die Mitarbeit an diesem Leitfaden danken wir daher herzlich folgenden Personen

- Phillip Fischer | scope & focus Service-Gesellschaft mbH
- Dr. Philipp Haas | Robert Bosch GmbH
- Dr. Ricarda Pantze | Deutsche Telekom AG
- Dr. Dominik Rabe | Rewe Zentralfinanz eG
- Christian Rein | Rechtsanwalt und Fachanwalt für Informationstechnologierecht
- Dr. Harald Schöning | Software AG
- Martin Schweinoch | SKW Schwarz Rechtsanwälte
- Maximilian Störzer | Stadtwerke München GmbH
- Dr. Matthias von Beckerath | Deutsche Telekom AG

Berlin, Januar 2021

1 Vgl. z. B. ↗ **Bitkom-Leitfaden »Open Data – Neue Konzepte erfolgreich umsetzen«**

Inhaltsverzeichnis

1 Erscheinungsformen von Daten (Was sind Daten?)

Für die juristische Betrachtung von »Daten« ist zunächst zwischen einer semantischen Ebene (Informationsgehalt der Daten) und einer technischen Ebene (Codierung auf dem Datenspeicher) zu unterscheiden. Aus technischer Sicht sind Daten maschinenlesbar codierte Werte, die als physikalischer oder elektronischer Zustand auf einem Datenträger gespeichert sind und zwischen Speichermedien übertragen werden können. Auf der semantischen Ebene fügen sich Daten zu Eigenschaftsangaben, Sachverhalten und Zusammenhängen, d. h. zu Informationen zusammen.

Kleinste informationstragende Einheit ist ein einzelnes Roh-Datum, also z. B. ein Mess- oder Zahlwert, eine Ortskennzeichnung, eine Laser- oder Sensorerfassung, ein Name. Ein Sinn und eine Bedeutung ergeben sich aus Einzeldaten allerdings erst durch ihre Verknüpfung und durch gegenseitigen Bezug in einem Datensatz. Einzeldaten müssen in Beziehung gesetzt werden zu einer Person, einem Objekt, einem Ereignis oder einem Ort. Nur so liefern sie Informationen z. B. zum Aufenthaltsort einer Person, zur Beschaffenheit eines Materials, zum Fertigungstakt einer Maschine oder zur Niederschlagsmenge an einem Ort. Diese Unterscheidung hat auch eine rechtliche Bedeutung. Die Frage nach dem rechtlichen Schutz für den Informationsgehalt von Daten führt in den Anwendungsbereich des geistigen Eigentums (Urheberrecht, gewerblicher Rechtsschutz). Unbefugte Veränderungen der Codierung auf einem Datenträger sind dagegen als Eingriff in das Sacheigentum am Datenträger anzusehen und damit sachenrechtlich und ggf. auch strafrechtlich relevant.

In rechtlichen Zusammenhängen sind des Weiteren personenbezogene und nicht personenbezogene Daten zu unterscheiden, da das Recht an den Umgang mit personenbezogenen Daten besondere Anforderungen stellt. Personenbezogene Daten sind definiert als »Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen« (Art. 4 Nr. 1 Datenschutz-Grundverordnung). In der Kategorie der personenbezogenen Daten bildet das Recht eine weitere Sonderkategorie besonders sensibler personenbezogener Daten, die Grundlage einer rechtlich missbilligten Diskriminierung sein können: Daten zu ethnischer Herkunft, politischer Meinung, religiöser Überzeugung, Gewerkschaftszugehörigkeit, Gesundheitszustand, Alter, sexueller Orientierung. Informationen in diesen Bereichen genießen sowohl im Datenschutzrecht als auch nach dem Allgemeinen Gleichbehandlungsgesetz (AGG) einen intensiveren Schutz. Diese differenzierte rechtliche Wertung ist auch bei der Verarbeitung von Daten z. B. in Big Data-Analysen und bei Anwendungen künstlicher Intelligenz zu berücksichtigen. Ggf. müssen die Daten bereits bei Erhebung entsprechend der zugehörigen Kategorie klassifiziert und geschützt werden.

Nicht personenbezogene Daten sind solche Daten, die sich nicht auf eine konkrete identifizierbare Person beziehen lassen. Dies können Daten über Tiere, Maschinen, Produkte, Umwelt- oder Naturzustände, Marktgegebenheiten oder auch anonymisierte Daten über Menschen sein. Für diese Arten von Daten gilt das Datenschutzrecht nicht, ihre Erhebung und Verarbeitung ist im Rahmen der allgemeinen Gesetze zulässig.

Während die Unterscheidung zwischen personenbezogenen Daten einerseits und nicht personenbezogenen Daten andererseits in der Theorie klar erscheint, ist sie in der Praxis vielfach nicht so eindeutig und verursacht teilweise erhebliche Rechtsunsicherheiten und Anwendungsschwierigkeiten.

Weitere Differenzierungen werden durch das Recht des geistigen Eigentums erforderlich. Dieses sieht einen besonderen rechtlichen Schutz vor für Daten, die in den Anwendungsbereich eines Leistungsschutzrechts fallen, und für Daten, deren Entstehung auf einem besonderen geistigen Schöpfungsakt beruht. Einen solchen Schutz genießen maschinengenerierte Rohdaten gerade nicht. Bei Rohdaten handelt es sich um Daten, die ohne direkten Einfluss eines Menschen durch Sensoren, Computer-Prozesse, Software oder Maschinen lediglich gesammelt, nach Erhebung aber noch nicht bearbeitet wurden.[2]

Im Wettbewerbsrecht wiederum erlangen marktrelevante Daten eine besondere rechtliche Bedeutung. Damit sind Daten gemeint, deren Zugang Voraussetzung für die Teilnahme an einem bestimmten Markt oder für ein bestimmtes Angebot ist oder die eine besondere Wettbewerbsposition begründen.

Schließlich kommt der Gegenleistung für eine Datenbereitstellung eine wichtige Bedeutung zu, sodass man Daten auch nach diesem Kriterium kategorisieren kann. Öffentlich zur allgemeinen Verfügung bereitgestellte Daten (»Open Data«) sind auch rechtlich nach anderen Vorgaben zu beurteilen als Daten, deren Erwerb von einer Gegenleistung abhängt.

2 Vgl. **↗ Mitteilung COM (2017) 9 final vom 10. Januar 2017 »Building a European Data Economy«**, S. 8, 9

2 Nutzungsmöglichkeiten von Daten (Was kann man mit Daten machen?)

2.1 Wertschöpfung durch Daten

Die Datenwertschöpfungskette reicht von der Erschließung von Datenquellen und dem Sammeln von Daten über die Speicherung von Daten, ihre Analyse und Auswertung, die Verknüpfung mit anderen Datenbeständen, die Herausfilterung bestimmter Datenmerkmale (z. B. Anonymisierung) bis hin zum Vergleich eines Datenbestandes mit Referenzdaten und zur Prüfung von Konsistenzen eines Datenbestandes. Ein Geschäftsmodell lässt sich aus der Verarbeitung von Daten dann machen, wenn dieser Verarbeitungsvorgang am Markt nachgefragt und vergütet wird.

Daten können in der digitalisierten Wirtschaft aber erst genutzt werden, wenn sie in elektronischer Form vorliegen, wenn also der oben unter Ziffer 1 beschriebene technische Datenbegriff erfüllt ist. Elektronisch vorliegende Daten können in vielfältiger Form weiterverarbeitet und nutzbar gemacht werden. Daten aus dem Unternehmen können z. B. für die Prozessoptimierung, für die Wartung von Maschinen und Anlagen, für Konstruktion und Design neuer Produkte oder für die Entwicklung gänzlich neuer Geschäftsmodelle genutzt werden. Daten über den Markt und das Kundenverhalten helfen beim Marketing, bei zielgenauer Kundenansprache und Produktplatzierung und bei der Verbesserung des Leistungsangebots.

2.2 Betrachtungsbeispiel: Automatisiertes Hochregallager

Die vielfältigen Möglichkeiten zur Nutzung von Daten, deren Einbeziehung in Wertschöpfungsprozesse und die rechtlichen Rahmenbedingungen hierfür sollen in diesem Leitfaden anhand des folgenden Praxisbeispiels erläutert werden: Ein Logistikunternehmen betreibt ein automatisiertes Hochregallager, in dem für verschiedene Kunden Artikel von unterschiedlicher Größe, in unterschiedlichen Behältnissen und mit unterschiedlichen Anforderungen an die Umgebungstemperatur eingelagert werden. Die Artikel werden auf Anweisung der jeweiligen Unternehmenskunden entweder für deren eigene Produktion oder für den Versand an deren Abnehmer bereitgehalten. Für die automatisierte Einlagerung der Artikel entsprechend den Vorgaben seiner Kunden nutzt das Logistikunternehmen elektrisch betriebene autonome Stapelroboter (»Paletten-Shuttles«). Das Logistikunternehmen präsentiert sich und sein Leistungsangebot auf einer eigenen Website.

Das Logistikunternehmen bietet seinen Kunden folgende Leistungen an:

- Einlagerung von Waren und Betriebsmitteln, bei Bedarf auch in Kühlräumen
- Annahme und Ausgabe von Waren und Betriebsmitteln
- Vorbereitung der eingelagerten Waren und Betriebsmittel zum Versand und zur Weiterlieferung (z. B. Etikettierung, Verpackung bzw. Abfüllung, Verladung).

Das Logistikunternehmen erhebt und verarbeitet folgende Daten:

- Daten zur Verfügbarkeit von Regallagerplätzen zur bestmöglichen Auslastung der Lagerfläche und für eine möglichst reibungslose Weiterlieferung
- Daten zur Verwaltung von leeren Paletten und Behältern (Daten zur Palettenauslastung, zum Palettenzustand und zur Palettenverfügbarkeit)
- Artikelnummern und Artikelbeschreibungen der eingelagerten Artikel sowie Angaben zur notwendigen Lagertemperatur
- Daten zur Erfassung und Verarbeitung von Aufträgen und Kundenanforderungen (Daten werden direkt aus den Kundensystemen übermittelt)
- Erfassung von Waren-, Versand- und Anlieferdaten für die Weiterlieferung, die Abrechnung gegenüber den Kunden und für steuerliche Zwecke
- Betriebs- und Servicedaten der Palettenshuttles (z. B. Batteriezustand, Sensor- und Kameradaten zur selbständigen Steuerung der Shuttles)
- Daten für eine Nachverfolgung von Lieferungen in Echtzeit
- Nutzerdaten von Besuchern der Firmen-Website.

3 Bestimmung des Datenwerts (Welchen Wert haben Daten?)

Daten sind für digitale Geschäftsmodelle unverzichtbar. Insoweit haben Daten für Unternehmen als Produktionsfaktor (neben Arbeit, Kapital und Rohstoffen / Energie) einen gewissen Wert. Der Wert von Daten liegt aber nicht in der Verfügbarkeit über einen möglichst großen Datenbestand, sondern in der Verbesserung ökonomischer Entscheidungen, die durch Analyse eines Datenbestandes möglich wird. Das bloße Sammeln und Speichern von Daten verursacht dagegen nur Kosten und bringt keinen Nutzen. Entsprechend können Daten auch nur bepreist werden, wenn und soweit aus ihnen Wertschöpfung generiert werden kann und es für diese Wertschöpfung einen Markt gibt.

3.1 Bewertung von Daten

Daten haben keinen Wert an sich. Erst Veredelungsprozesse wie Formatierung, Analyse, Vergleich, In-Beziehung-Setzen, Anreichern und Interpretieren im Hinblick auf ein konkretes Anwendungsszenario lassen aus einem Datenbestand nützliche und wertvolle Informationen entstehen. Der wirtschaftliche Wert von Daten hängt daher vor allem von ihrem Nutzen für ein Geschäftsmodell ab bzw. von der Möglichkeit, aus ihnen nutzbare und bepreisbare Informationen zu gewinnen. Als Indikator dafür, ob einem Datenbestand auch ein merkantiler Wert zukommt, kann der Wirtschaftsgutbegriff des Steuerrechts herangezogen werden. Ein Wirtschaftsgut ist eine Sache, ein Recht oder ein tatsächlicher Zustand, eine konkrete Möglichkeit oder ein Vorteil für den Betrieb, deren Erlangung sich der Kaufmann etwas kosten lässt, die einer besonderen Bewertung zugänglich sind und zumindest mit dem Betrieb übertragen werden können.[3] Der merkantile Wert von Daten ist danach abhängig vom Nutzwert der Daten für ein Unternehmen und von der Marktfähigkeit von Daten. Sowohl der volle Nutzwert als auch die Marktfähigkeit setzen voraus, dass die Daten von ihrem Inhaber ohne rechtliche Einschränkungen verwendet und weitergegeben werden können.[4] Für die Marktfähigkeit ist darüber hinaus erforderlich, dass andere Marktakteure als der Datenerzeuger ein Interesse an der Abnahme der Daten haben.

3 Begriff des »Wirtschaftsguts« in ↗ **Hinweis 4.2 Abs. 1 der Einkommensteuer-Richtlinien**

4 Auch der BGH erkennt an, dass ein Datenbestand ein vermögenswertes Gut darstellen kann, wenn er gegen Entgelt veräußert werden kann (BGH, Urteil vom 2.7.1996 – X ZR 64 / 94).

3.2 Wert von personenbezogenen Daten

Ein Wert wird Daten teilweise nicht nur dann zugemessen, wenn sie gegen ein Entgelt zur Nutzung übertragen werden, sondern auch dann, wenn sie hingegeben werden, um eine ansonsten kostenfreie Leistung (z. B. Vernetzung über eine Social Media Plattform) in Anspruch nehmen zu können (»Daten als Gegenleistung« oder »Daten als Entgelt«). Bei den hingegebenen Daten handelt es sich dabei um personenbezogene Daten als Gegenleistung für ansonsten kostenfreie Services.

Die Rechtsprechung sieht in der Hingabe personenbezogener Daten aber keine Übertragung eines Vermögenswertes. »Denn die Herausgabe personenbezogener Daten bzw. die datenschutzrechtlich erforderliche Einwilligung in deren Erhebung und Verarbeitung beeinträchtigt den Verbraucher ›lediglich‹ in seinen rein immateriellen Interessen, nämlich in seinem Recht auf informationelle Selbstbestimmung. Unmittelbare finanzielle Einbußen sind für ihn damit nicht verbunden.«[5] Der Schutz personenbezogener Daten bezweckt vor allem den Schutz der dahinter stehenden Persönlichkeit und dient damit der Durchsetzung eines verfassungsrechtlichen Gebots. Bei einer wirtschaftlichen Nutzung personenbezogener Daten als Gegenleistung für den Zugang zu Gütern und Dienstleistungen besteht die Gefahr, dass die geschützte Person den Schutz ihrer personenbezogenen Daten und damit einen Teil ihres Persönlichkeitsschutzes aufgibt, um die Gegenleistung erhalten zu können. Auch ist die Hingabe personenbezogener Daten kaum als gleichwertige Gegenleistung anzuerkennen, soweit die betroffene Person von der in der DS-GVO vorgesehenen Befugnis zum Widerruf der Einwilligung in die Datenverarbeitung Gebrauch machen kann.

Dennoch erkennt das Recht in einzelnen Bereichen der Hingabe personenbezogener Daten eine gewisse wirtschaftliche Gleichwertigkeit mit anderen vertraglichen Leistungen zu. So ist in der Richtlinie (EU) 2019/770 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen ausdrücklich festgehalten, dass Verbrauchern bei Hingabe ihrer personenbezogene Daten im Rahmen einer ansonsten unentgeltlichen Leistung dieselben Rechte zustehen wie bei einer entgeltlichen Leistung. Dies gilt nur dann nicht, wenn die personenbezogenen Daten vom Unternehmer ausschließlich für die Zwecke der Erfüllung des Vertrages verwendet werden dürfen.

Aus Sicht der Unternehmen, die an personenbezogenen Daten interessiert sind, ist die durch die DS-GVO vorgesehene Widerrufsmöglichkeit der Einwilligung in die Nutzung von personenbezogenen Daten ein großes Problem. Findet eine Datenverwendung auf Grundlage der Einwilligung des Betroffenen statt, kann der Betroffene durch seinen Widerruf die Rechtsgrundlage der Datenverwendung entziehen. Problematisch ist hier, dass sich nach Auffassung einiger Aufsichtsbehörden der Datenverarbeiter eine Verarbeitungsgrundlage aussuchen muss, also nicht auf Einwilligung und zusätzlich auf eine gesetzliche Grundlage (z. B. Verarbeitung zur Vertragserfüllung) setzen darf. Dies schränkt die Planungssicherheit der Unternehmen und den Anreiz für innovative Datennutzungskonzepte ein. Der Wert personenbezogener Daten sinkt rapide, wenn Unternehmen damit rechnen müssen, die Nutzung jederzeit wieder einstellen zu müssen.

5 LG Berlin, Urteil vom 16.1.2018, Az. 16 O 341/15; nicht rechtskräftig

3.3 Wert von Maschinendaten

Maschinendaten gewinnen vor allem dann einen besonderen Wert, wenn Geschäftsmodelle digitalisiert werden und Daten zur Geschäftsgrundlage werden. So lässt sich z. B. das Geschäftsmodell »Verkauf einer Maschine« in das Geschäftsmodell »Angebot von Maschinenleistungen« umwandeln. Dem Kunden wird in diesem Fall ein Service angeboten, der in der Bereitstellung von möglichst reibungslos nutzbaren Maschinenleistungen besteht (pay per use). Damit der Anbieter hierbei seine Service Levels erfüllen kann, nutzt er regelmäßig predictive maintenance. Er analysiert also fortwährend die von der Maschine generierten Betriebsdaten und leitet eine Wartung ein, wenn sich eine Schlechtleistung oder ein Ausfall der Maschine andeutet.

4 Gesetzlicher Schutz von Daten (Wie sind Daten gesetzlich geschützt?)

Bereits im Grundgesetz ist ein gewisser Schutz für Daten und für die Nutzung von Daten angelegt. Aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG wird ein Recht auf informationelle Selbstbestimmung als Element des Allgemeinen Persönlichkeitsrechts abgeleitet. Danach hat jede natürliche Person das Recht, über die Verwendung von Daten von und über sich selbst zu bestimmen. Ein Geheimnisschutzrecht für betriebliche Informationen wird als Ausfluss von Art. 19 Abs. 3 oder Art. 14 Abs. 1 GG bzw. Art. 12 Abs. 1 GG inländischen juristischen Personen zugesprochen.[6] Zwar handelt es sich hierbei um Abwehrrechte gegen den Staat. Doch die Vorgabe zur Erfüllung grundrechtlicher Schutzpflichten begründet auch die Veranlassung für den Staat, gesetzliche Regelungen zu schaffen, die den im GG vorgegebenen Schutz durchsetzen und Schranken für die Verwendung von Daten auch zwischen Privaten setzen.[7] Dieser Pflicht ist der Gesetzgeber mit verschiedenen Gesetzen bzw. gesetzlichen Regelungen nachgekommen.

4.1 Datenschutz

Die Datenschutz-Grundverordnung (DS-GVO) und ergänzende nationale Vorschriften gewähren einen besonderen Schutz für personenbezogene Daten i. S. d. Art. 4 Nr. 1 DS-GVO, d. h. für Informationen über eine natürliche Person, ihre Aktivitäten, ihren Aufenthaltsort und ihre Kontakte. Begünstigter dieses Rechtsschutzes ist die betroffene Person, also das Bezugssubjekt der Daten. Der Schutz ist so umgesetzt, dass für datenverarbeitende Stellen (z. B. Behörden und Unternehmen) die Verarbeitung personenbezogener Daten (z. B. Erhebung, Speicherung, Analyse) grundsätzlich verboten und nur auf der Grundlage eines Erlaubnistatbestands nach Art. 6 DS-GVO zulässig ist. Wird allerdings der konkrete Personenbezug durch Anonymisierung entfernt oder liegt kein Personenbezug vor, findet das Datenschutzrecht keine Anwendung.[8]

Im oben (unter Ziffer 2.2) skizzierten Betrachtungsbeispiel wären die Daten zu Kundenaufträgen genauso wie Versand- und Lieferdaten und die Abrechnungsdaten als personenbezogene Daten zu qualifizieren. Dies gilt jedoch nur, soweit es sich bei den jeweiligen Kunden um natürliche Personen handelt, da die DS-GVO keinen Datenschutz für juristische Personen begründet. Die Daten zur Nutzung der Firmen-Website sind als personenbezogene Daten anzusehen. Die Daten für eine Nachverfolgung von Lieferungen in Echtzeit sind dann personenbezogen, wenn sie Identifikationsmerkmale von natürlichen Personen umfassen.

6 BVerfG, Beschluß vom 14.03.2006, Az. 1 BvR 2087/03; BGH, Urteil vom 08.02.1994, Az. VI ZR 286/93; Michalski / Funke, in: Michalski, GmbHG, 2. Aufl. 2010, § 13 Rn. 566.

7 Di Fabio, in Maunz / Dürig, Grundgesetz-Kommentar, 66. Erg.Lfg. 2012, Rn. 189 f. m.w.N.

8 Vgl. zu rechtlichen und technischen Anforderungen an eine wirksame Anonymisierung den **↗ Bitkom-Leitfaden zur »Anonymisierung und Pseudonymisierung von Daten für Projekte des maschinellen Lernens«** sowie den **↗ BDI-Praxisleitfaden »Anonymisierung personenbezogener Daten«**

4.2 Schutz als geistiges Eigentum

Das Recht des geistigen Eigentums (z. B. Halbleiterschutzgesetz, Designgesetz, Urheberrechtsgesetz, Patentgesetz) bietet einen gesetzlichen Schutz für immaterielle Güter (z. B. Konzepte, Ideen, Computersoftware). Damit sollen demjenigen, der das jeweilige immaterielle Gut erfunden bzw. entwickelt hat, eine vorrangige wirtschaftliche Verwertung seiner Schöpfung und seiner Investitionen sowie ein Schutz vor Nachahmung gesichert werden. Der gesetzliche Schutz des geistigen Eigentums greift jedoch regelmäßig nicht für einzelne Informationen. So gilt das Leistungsschutzrecht an Datenbanken (§§ 87a ff. UrhG) nur bei Kopie der gesamten Datenbank oder wesentlicher Teile davon, nicht für einzelne Datensätze.[9] Auch sind Investitionen in die Erzeugung von Daten, die im Anschluss in der Datenbank dargestellt werden, nicht vom Datenbankherstellerrecht umfasst.[10] Datenbestände, die lediglich als Nebenprodukt eines Geschäftsbetriebs anfallen, sollen ebenfalls nicht dem Datenbankschutz unterfallen.[11]

Der Schutz des Urhebers nach §§ 2 Abs. 2, 4 Abs. 2 UrhG umfasst lediglich strukturgebende Ideen oder Werke von einer gewissen Schöpfungshöhe. Auf einzelne Daten erstreckt sich dieser Schutz nicht. Denn der Erzeugung einzelner Daten (insbesondere bei automatisierter Erzeugung durch Sensoren oder Messeinrichtungen) liegt regelmäßig kein persönlich geistiger Schöpfungsakt zugrunde. Teilweise ist die Begrenzung des Rechtsschutzes auf eine neuartige Idee und ihre technische Umsetzung im jeweiligen Schutzgesetz selbst geregelt. So erstreckt sich der Halbleiterschutz nach § 1 Abs. 4 HalblSchG ausdrücklich nicht auf die auf einem Halbleiter gespeicherten Informationen.

Inhalt des Patentschutzes nach § 9 Nr. 3 PatG ist das alleinige Recht des Patentinhabers, durch ein patentgeschütztes Verfahren hergestellte Erzeugnisse anzubieten, in Verkehr zu bringen oder zu gebrauchen oder zu den genannten Zwecken entweder einzuführen oder zu besitzen. Eine bestimmte Datenfolge kann Erzeugnis in diesem Sinn sein. Als solches ist ihre Verwertung vom Patentschutz umfasst, wenn die Datenfolge sachlich-technische Eigenschaften aufweist, die ihr durch das patentgeschützte Verfahren aufgeprägt wurden. Ein Datenbestand, der lediglich die erfindungsgemäß gewonnenen Erkenntnisse enthält, fällt dagegen nicht unter den Patentschutz.[12]

Das Betrachtungsbeispiel (oben unter Ziffer 2.2) wurde so gebildet, dass für die anfallenden Informationen ein Schutz als geistiges Eigentum ausscheidet.

---

9 Vgl. ↗ **EuGH, Urteil vom 09.11.2004 (Rs. C-203/02 »The British Horseracing Board«)**, Rn. 69ff., und OLG Hamburg, Urteil vom 24.10.2012, Az. 5 U 38/10

10 ↗ **EuGH, Urteil vom 09.11.2004 (Rs. C-203/02 »The British Horseracing Board«)**, Rn. 38 – 42 und ↗ **EuGH, Urteil vom 09.11.2004 (Rs. C-444/02 »Fixtures Marketiung«)**, Rn. 53

11 Vgl. z. B. ↗ **BGH, Urteil vom 01.12.2010, Az. I ZR 196/08**, Rn. 35, sowie zu diesem Themenkomplex auch die Erörterung von Hornung / Hofmann in: Hornung (Hrsg.): »Rechtsfragen der Industrie 4.0«, Nomos 2018, S. 25 mit Hinweis auf ↗ **EuGH, Urteil vom 09.11.2004 (Rs. C-338/02 »Fixtures-Fußballspielpläne«)**

12 Vgl. ↗ **BGH, Urteil vom 27.09.201 , Az. X ZR 124/15**, und BGH, Urteil vom 21.08. 2012, Az. X ZR 33/10 (Videosignal-Codierung)

4.3 Schutz von Geschäftsgeheimnissen

Nach dem Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG), das die Richtlinie (EU) 2016 / 943 in deutsches Recht umsetzt, sind vertrauliche Unternehmensinformationen als Geschäftsgeheimnisse geschützt, wenn das Unternehmen angemessene Maßnahmen zur Geheimhaltung dieser Informationen getroffen hat. Auf diese Weise hat es ein Unternehmen weitgehend selbst in der Hand, welche Informationen als Geschäftsgeheimnis dem gesetzlichen Schutz unterfallen. Allerdings sieht das Gesetz nur einen möglichen Schutz von Informationen vor, einzelne Rohdaten wären damit wohl nicht vom Schutzbereich erfasst.

Gesetzlich geschützt ist vor allem die Vertraulichkeit von Geschäftsgeheimnissen. Eine »Wissensexklusivität« soll dem Inhaber des Geschäftsgeheimnisses die ungestörte profitable Nutzung eigener Innovationsaktivitäten und des damit erarbeiteten Informationsvorsprungs sichern. Entsprechend sind der unbefugte Zugang und das unbefugte Kopieren von Geschäftsgeheimnissen verboten (§§ 4, 23 GeschGehG). Bei Verletzung seines Geschäftsgeheimnisses kann der Inhaber sowohl gegen denjenigen vorgehen, der das Geheimnis unberechtigt kopiert oder offengelegt hat, als auch gegen Dritte, die das Geheimnis im Anschluss unbefugt nutzen (§§ 6 ff. GeschGehG). Dabei sind die Rechte des Geheimnisinhabers umfassend, sie reichen von Auskunftsrechten über Rechte auf Unterlassung, Herausgabe bzw. Löschung bis zu Schadensersatzansprüchen. Allerdings dürfen produktimmanente Informationen durch Untersuchung frei auf dem Markt verfügbarer Produkte aufgedeckt (Reverse Engineering) und in der Folge weiter verwendet werden (§ 3 Abs. 1 Nr. 2 GeschGehG). Insoweit liegt keine Verletzung eines Geschäftsgeheimnisses vor.

Die Daten im Betrachtungsbeispiel (oben unter Ziffer 2.2) sind nicht per se als Geschäftsgeheimnisse des Logistikunternehmens geschützt. Denn zur Begründung eines solchen Schutzes müsste das Logistikunternehmen geeignete Schutzmaßnahmen gegen unberechtigten Zugriff auf die Daten und gegen deren unberechtigte Offenlegung ergreifen. Als solche Maßnahmen kommen vertragliche Abreden mit Geschäftspartnern, aber auch physische Zugangsbeschränkungen sowie interne Richtlinien und Regelungen in Arbeitsverträgen in Betracht. Fraglich ist, ob bereits die Sensordaten der Palettenshuttles als reine Roh-Daten Gegenstand eines Geschäftsgeheimnisses sein können.

Allerdings verarbeitet das Logistikunternehmen auch Daten seiner Geschäftspartner (z. B. Abrechnungsdaten, Auftragsdaten, Lieferdaten), die teilweise direkt aus den EDV-Systemen der Kunden stammen. Bei diesen Drittdaten handelt es sich um Geschäftsgeheimnisse der Geschäftspartner, wenn diese ihrerseits Maßnahmen zum Schutz gegen unberechtigten Zugriff auf diese Daten getroffen haben. Ist dies der Fall, hat das Logistikunternehmen insbesondere die vertraglichen Vorgaben seiner Geschäftspartner bei Verarbeitung und Nutzung der Daten zu beachten. Außerdem sollte das Logistikunternehmen Daten, die als Geschäftsgeheimnisse seiner Geschäftspartner anzusehen sind, vertraulich behandeln, um keine Sanktionen nach dem Geschäftsgeheimnisgesetz befürchten zu müssen.

4.4 Sachenrechtlicher Schutz

Im geltenden Zivilrecht genießt der Eigentümer einer Sache einen umfassenden Rechtsschutz. Nach § 903 S. 1 BGB berechtigt das Eigentum an einer Sache den Eigentümer, mit der Sache nach Belieben zu verfahren, die Bedingungen für die Nutzung der Sache zu bestimmen und andere Personen von einer Einwirkung auf die Sache auszuschließen. Die eigentumsrechtlichen Vorschriften des BGB (§§ 903 ff. BGB) sind jedoch für körperliche Gegenstände (Sachen) konzipiert und daher für unkörperliche Gegenstände wie Daten nicht anwendbar.[13] Gegen eine Anwendung der Vorschriften zum Sacheigentum auf Daten spricht letztlich vor allem das Wesen von Daten als nicht-rivale, nicht-exklusive und nicht-abnutzbare Gegenstände. Das Sachenrecht für bewegliche Sachen wurde dagegen geschaffen für eine exklusive Zuordnung von nicht beliebig multiplizierbaren Gegenständen, die durch Nutzung an Wert verlieren. Aus ähnlichen Erwägungen hat die Rechtsprechung auch die Anwendung der Besitzschutzvorschriften (§§ 854 ff. BGB) auf Daten abgelehnt.[14]

Das Sacheigentum des BGB umfasst allerdings den Schutz von Datenträgern, da diese wiederum Sachen sind. Über den Eigentumsschutz an Datenträgern sind die darauf gespeicherten Daten mittelbar mitgeschützt. Die unbefugte Änderung oder Löschung von Daten ist daher als Eingriff in das Eigentum am Datenträger anzusehen, der zu Schadensersatz führen kann (z. B. nach § 823 Abs. 1 BGB), wenn die Nutzungs- und Verfügungsmöglichkeiten des Berechtigten über Daten und Datenträger (Integritätsinteresse) durch den unbefugten Eingriff beeinträchtigt sind.[15] Die bloße Kenntnisnahme oder das bloße Kopieren von Daten ohne deren Veränderung ist allerdings kein Eingriff in das Eigentum am Datenträger. Denn das bloße Kopieren beeinträchtigt die Integrität und die Nutzbarkeit von Daten und Datenträger nicht.

Das Logistikunternehmen könnte sich im oben (unter Ziffer 2.2) geschilderten Betrachtungsbeispiel für die von ihm erhobenen und verarbeiteten Daten nur dann auf einen sachenrechtlichen Schutz berufen, wenn ein Dritter den vorhandenen Datenbestand verändert oder darin Löschungen vornimmt.

13 So auch das LG Konstanz (vgl. Urteil vom 10.05.1996, Az. 1 S 292/95)

14 ↗ **OLG Brandenburg, Urteil vom 06.11.2019, Az. 4 U 123/19**

15 So z. B. OLG Karlsruhe, Urteil vom 07.11.1995, Az.3 U 15/95

4.5 Strafrechtsschutz

Das Strafrecht gewährt einen Schutz vor unberechtigtem Zugriff auf einen Datenbestand nach §§ 202a, 202b, 202c StGB. Danach ist es verboten, Einrichtungen zum Schutz von Daten (z. B. Firewall oder Verschlüsselung) zu umgehen, um Zugriff auf die Daten zu erlangen. Die Vorschriften der §§ 303a und 303b StGB verbieten die unberechtigte Löschung, Veränderung, Beschädigung und Zerstörung von Daten. Geschütztes Rechtsgut der Strafvorschriften ist die Datenintegrität und die ungehinderte Verfügungsmöglichkeit des Berechtigten über Daten, nicht aber die rechtliche Zuordnung von Daten oder die Vertraulichkeit einer Information. Das bloße Kopieren von nicht besonders gegen Zugriff gesicherten Daten ist daher nicht Tathandlung. Auch ist der Integritätsschutz des Strafrechts für einen Datenbestand nicht lückenlos; denn fahrlässige Veränderungen von Datenbeständen sind nicht von den Datenstraftatbeständen erfasst.

Der strafrechtliche Schutz steht jedem berechtigten Dateninhaber zu. Berechtigter Dateninhaber ist derjenige, der die Speicherung von Daten unmittelbar durch Eingabe, durch Start eines Speicherprogramms oder durch bestimmungsgemäße Verwendung eines zur Datenerzeugung und -aufzeichnung bestimmten Gerätes bewirkt hat. Allein aus der Herstellung und dem Verkauf eines Gerätes zur Datenerzeugung kann – wenn eine entsprechende Vereinbarung fehlt – eine Berechtigung an den damit erzeugten Daten nicht abgeleitet werden.[16]

Sind Strafvorschriften einschlägig, kann ein unbefugter Zugriff auf die mit den Strafvorschriften geschützten Rechtsgüter auch zivilrechtlich nach § 1004 BGB analog abgewehrt bzw. nach § 823 Abs. 2 BGB mit einem Anspruch auf Schadensersatz verfolgt werden.

Ähnlich wie beim sachenrechtlichen Schutz greift auch der Strafrechtsschutz für die Daten des Logistikunternehmens nur ein, wenn der bei ihm vorhandene Datenbestand durch unbefugte Dritte in irgendeiner Weise verändert wird oder wenn Vorrichtung zum Schutz der Daten gezielt umgangen werden.

16 ↗ OLG Naumburg, Urteil vom 27.08.2014, Az. 6 U 3/14

4.6 Konsequenzen für die Praxis

Das geltende Recht kennt einen besonderen rechtlichen Schutz nur für bestimmte Kategorien von Informationen. Maschinengenerierte Einzeldaten sind daher nicht gesetzlich geschützt. Einen gesetzlichen Schutz des Dateninhabers kennt das deutsche Recht nur als Integritätsschutz für einen Datenbestand oder bei Begründung von Geschäftsgeheimnissen oder – in Ausnahmefällen – als Reflex eines Rechts an geistigem Eigentum oder am Sacheigentum des Datenträgers. Eine Ausschließlichkeitsstellung für Daten lässt sich aus dem geltenden deutschen Recht nicht ableiten.

Daraus ergibt sich zum einen, dass für die Erhebung und Verarbeitung von Daten weitreichende Möglichkeiten bestehen, solange die jeweiligen rechtlichen Schranken (dazu sogleich unter 5.) eingehalten werden. Da ein gesetzlicher Schutz für Daten und Informationen, die im Unternehmen erhoben werden, nur in wenigen Fällen bei Erfüllung besonderer Voraussetzungen besteht, bietet es sich zum anderen an, einen Schutz wertvoller Daten gegenüber Geschäftspartnern über Verträge zu etablieren.

In Verträgen kann auch festgelegt werden, dass und unter welchen Bedingungen ein im Einzelfall anzuerkennendes Schutzrecht an Daten zugunsten des Vertragspartners aufgegeben wird. Wenn also z. B. der Inhaber einer Datenbank seinem Vertragspartner das Recht einräumt, beliebige Datensätze aus der Datenbank zu kopieren, kommt es nicht mehr darauf an, welche Datensätze in der Datenbank vom gesetzlichen Datenbankschutz erfasst werden.

5 Gesetzliche Restriktionen der Datennutzung (Was darf man mit Daten machen?)

Auch wenn das geltende deutsche Recht kein eigenständiges Dateneigentum kennt, ist der Umgang mit Daten in vielerlei Hinsicht rechtlich vorgeprägt und von rechtlichen Schranken eingehegt. Wesentliche gesetzliche Grenzen und Vorgaben für Datenzugang und Datennutzung werden im Folgenden kurz dargestellt.

5.1 Datenschutz

Wie bereits erwähnt gilt im Datenschutzrecht das Verbot mit Erlaubnisvorbehalt, d. h. die Verarbeitung personenbezogener Daten ist nur dann rechtmäßig, wenn für den konkreten Verarbeitungsvorgang eine Erlaubnis der betroffenen Person oder ein gesetzlicher Ermächtigungstatbestand vorliegt. Die gesetzlichen Ermächtigungstatbestände sind in der unmittelbar geltenden DS-GVO abschließend geregelt. Danach ist z. B. die Verarbeitung personenbezogener Daten zulässig zur Erfüllung eines Vertrages durch den Vertragspartner der betroffenen Person (Art. 6 Abs. 1a DS-GVO) oder bei Vorliegen berechtigter Interessen des Verantwortlichen oder eines Dritten (Art. 6 Abs. 1f) DS-GVO). Für Unternehmen sind die abstrakt formulierten Erlaubnistatbestände mit erheblicher Rechtsunsicherheit verbunden, die schwer hinzunehmen ist, wenn datengetriebene Innovationen ermöglicht werden sollen.[17]

Auch für eine zulässige Datenverarbeitung auf der Grundlage einer einschlägigen Ermächtigungsgrundlage sind weitergehende Anforderungen und Vorgaben der DS-GVO zu beachten. Die Datenverarbeitung ist gegen den Zugriff unbefugter Dritter durch geeignete Maßnahmen abzuschirmen. Für die Erfüllung von Rechten der betroffenen Person, z. B. Informationsrechte, Anspruch auf Datenübertragung, auf Einschränkung der Datenverarbeitung oder auf Löschung der Daten, ist Sorge zu tragen. Der deutsche Gesetzgeber hat im Übrigen von der Ermächtigung in Art. 6 Abs. 2 DS-GVO Gebrauch gemacht und spezifischere, die Ermächtigungsgrundlagen der DS-GVO konkretisierende Bestimmungen in dem in 2017 neugefassten Bundesdatenschutzgesetz (BDSG) erlassen. Unternehmen können den Geltungsbereich der DS-GVO und damit deren Vorgaben an die Datenverarbeitung verlassen, soweit sie Daten nur in anonymer Form erheben oder in zulässiger Weise anonymisierte Daten verarbeiten.[18]

Soweit das Logistikunternehmen im Betrachtungsbeispiel personenbezogene Daten verarbeitet, die ihm von seinen Geschäftspartnern übermittelt werden, wird es als Auftragsverarbeiter tätig.

17 Peitz / Schweitzer: »Ein neuer europäischer Ordnungsrahmen für Datenmärkte?«, in: NJW 2018, 275, 276 ff. für die Erlaubnistatbestände in Art. 6 Abs. 1a und Abs. 1f) DS-GVO

18 Vgl. zu rechtlichen und technischen Anforderungen an eine wirksame Anonymisierung den **↗ Bitkom-Leitfaden zur »Anonymisierung und Pseudonymisierung von Daten für Projekte des maschinellen Lernens«** sowie den **↗ BDI-Praxisleitfaden »Anonymisierung personenbezogener Daten«**

Für diese Tätigkeit verlangt die DS-GVO den Abschluss einer besonderen Vereinbarung zur Auftragsverarbeitung.[19] Die Erhebung von personenbezogenen Daten über die Homepage ist in der Regel nur rechtmäßig, wenn die betroffenen Personen dazu ihre Einwilligung gegeben haben oder wenn das Logistikunternehmen für die Datenerhebung ein berechtigtes Interesse (z. B. Sicherstellung der generellen Funktionsfähigkeit einschließlich IT-Sicherheit) geltend machen kann.

5.2 IT- Sicherheit

Die IT-Sicherheit dient dazu, Vertraulichkeit, Integrität und Verfügbarkeit von Informationen im Unternehmen zu gewährleisten. Insoweit wird ein Unternehmen auch ohne konkrete gesetzliche Vorgaben ein Eigeninteresse daran haben, Schutzmaßnahmen gegen unbefugte Zugriffe auf seine Datenverarbeitungssysteme und die damit verarbeiteten Daten zu etablieren. Teilweise greift auch der gesetzliche Schutz für Daten (z. B. im Strafrecht oder nach Geschäftsgeheimnisschutzgesetz) nur ein, wenn der Dateninhaber Maßnahmen zum Schutz seiner Daten vor unberechtigtem Zugriff ergriffen hat.

Für besonders sensible Daten (z. B. Gesundheitsdaten) verbietet das Gesetz jedoch auch explizit, dass diese Daten offenbart und Unbefugten zugänglich gemacht werden (vgl. z. B. § 203 StGB). Daraus ergeben sich besondere, erhöhte Sorgfaltsanforderungen und Verantwortlichkeiten für diejenigen, die mit diesen Daten umgehen. Werden personenbezogene Daten verarbeitet, müssen die Schutzmaßnahmen zur IT-Sicherheit zumindest den Anforderungen des Datenschutzes entsprechen. Wird der vom Gesetz verlangte Sorgfaltsmaßstab nicht beachtet, drohen Strafen und Bußgelder.

Für Unternehmen, die Teil einer Kritischen Infrastruktur sind, gelten spezialgesetzliche Vorschriften zur IT-Sicherheit. Diese sind in unterschiedlichen Gesetzen und Verordnungen geregelt, insbesondere hervorzuheben sind IT-Sicherheitsgesetz und Telekommunikationsgesetz. Beide Gesetze werden derzeit umfassend überarbeitet. Welche Unternehmen als kritische Infrastruktur eingestuft werden, ergibt sich aus der KRITIS-VO. Für Telekommunikationsunternehmen ergeben sich spezielle Anforderungen aus dem Sicherheitskatalog gemäß §109 Abs. 6 TKG. Für sonstige Kritische Infrastrukturen ergeben sich Sicherheitsanforderungen aus § 8a BSIG.

Vorgaben der IT-Sicherheit können dem Dateninhaber nahelegen, seinen Datenbestand gegen unberechtigten Zugriff Dritter zu schützen. Eine Beseitigung des Zugriffsschutzes im Einzelfall für berechtigten Datenzugriff wäre dann auf vertraglicher Grundlage zu regeln.

19 Ein Muster für eine Vereinbarung zur Auftragsverarbeitung ist auf der ↗ **Bitkom-Themenseite zur DS-GVO** zu finden.

5.3 Kartellrecht

Nach Art. 101 Abs. 1 AEUV, § 1 GWB sind Vereinbarungen zwischen Unternehmen und aufeinander abgestimmte Verhaltensweisen verboten, die eine Verhinderung, Einschränkung oder Verfälschung des Wettbewerbs bezwecken oder bewirken. Ein regelmäßiger, evtl. sogar automatisierter Datenaustausch zwischen Markteilnehmern wird von diesem Verbot erfasst, wenn es sich dabei um den Austausch wettbewerblich sensibler Informationen handelt. In den vergleichsweise noch jungen Datenmärkten gibt es vielfach noch Schwierigkeiten bei der Bestimmung wettbewerblich sensibler Informationen, bei der Identifizierung potenzieller Wettbewerber oder bei der Marktabgrenzung. Auch ist unklar, wie Vorkehrungen ausgestaltet sein müssen, um die Übermittlung bzw. den Empfang wettbewerblich sensibler Daten zu verhindern.

Allerdings reicht der bloße Austausch von Informationen und eine daraus folgende Abstimmung nicht zur Begründung eines kartellrechtlich verbotenen abgestimmten Verhaltens i. S. d. § 1 GWB aus. Hinzukommen muss ein konkretes Verhalten zur Umsetzung der Abstimmung, das auf eine Beeinflussung des Wettbewerbs gerichtet ist.[20]

Sofern Daten von mehreren Wettbewerbern genutzt werden sollen (z. B. für statistische Auswertungen), ist sicherzustellen, dass wettbewerbsrelevante Daten nur anonymisiert, d. h. vor allem aggregiert, verwendet werden. Daher sollte eine solche Datennutzung immer über eine neutrale Stelle erfolgen, die gewährleistet, dass über die Daten ein Rückschluss auf das Marktverhalten einzelner Wettbewerber nicht möglich ist.

Auch kann eine große Datenmacht zu einer wettbewerbsbeherrschenden Stellung führen und mit entsprechenden kartellrechtlichen Konsequenzen (verstärkte Beobachtung, Missbrauchsaufsicht) einhergehen. Diese Konsequenzen können bis zur Untersagung einer Datenerhebung in bestimmten Fällen reichen.[21] Eine weitere Konsequenz aus einer großen Datenmacht eines Unternehmens auf einem Markt kann darin bestehen, dass das Unternehmen anderen Unternehmen Zugang zu seinen Daten gewähren muss. Hierbei müssen jedoch zusätzlich zur besonderen Marktmacht des verpflichteten Unternehmens weitere Voraussetzungen erfüllt sein.[22]

In dem für diesen Leitfaden gewählten Beispielsfall (vgl. oben Ziffer 2.2) sind kartellrechtliche Aspekte nicht zu berücksichtigen.

20 BGH, Beschl. v. 13.7.2020, Az. KRB 99/19

21 Vgl. z. B. ↗ **Beschluss des Bundeskartellamtes B6-22/16 vom 6. Februar 2019**

22 Vgl. zu weiteren Einzelheiten die ↗ **Bitkom-Stellungnahme »Rechtsfragen der digitalisierten Wirtschaft: Datenrechte«**

5.4 Branchenspezifische Anforderungen

Zusätzlich zu den dargestellten allgemeinen rechtlichen Grenzen der Datenverarbeitung, die im Wesentlichen für alle Branchen in gleicher Weise gelten, sieht das Recht für Unternehmen bestimmter Branchen, z. B. die Finanz- und Versicherungswirtschaft und das Gesundheitswesen, weitergehende Vorgaben und Einschränkungen der Datenverarbeitung vor. Diese Vorgaben sollen vor allem einen erhöhten Standard für die IT-Sicherheit durchsetzen, da in den genannten Branchen in größerem Umfang Informationen verarbeitet werden, die vom Gesetzgeber als besonders sensibel eingestuft werden. Darüber hinaus gelten spezialgesetzliche Regelungen für Diensteanbieter im Telemedienbereich z. B. in §§ 88 ff. TKG oder – stark eingeschränkt – in §§ 11 ff. TMG.

Diese spezialgesetzlichen Vorgaben sind jedoch im hier gewählten Betrachtungsbeispiel (oben Ziffer 2.2) nicht einschlägig.

5.5 Ausblick auf künftige Gesetzgebung

Die Bedeutung von Daten für Wirtschaft und Gesellschaft findet zunehmend ihren Niederschlag in der Gesetzgebung sowohl auf nationaler als auch auf europäischer Ebene. Mit der Datenschutzgrundverordnung (DS-GVO) gelten in der EU bereits weitgehend einheitliche Regeln für die Verarbeitung personenbezogener Daten. Damit ist die Rechtsentwicklung aber nicht abgeschlossen. So enthält der **↗ Vorschlag eines Data Governance Act** der EU-Kommission u. a. Bedingungen für die Nutzung von Daten des öffentlichen Sektors, Anforderungen an Datentreuhänder, die eine Vermittlerrolle im Datenaustausch zwischen Verbrauchern und vertrauenswürdigen Institutionen einnehmen sollen, und Vorgaben für Organisationen, die freiwillig bereitgestellte Daten (Datenspenden) in Empfang nehmen. Der **↗ Vorschlag der EU-Kommission für einen Digital Markets Act** sieht bestimmte Beschränkungen der Datenhaltung für große Online-Plattformen vor (z. B. Offenhaltung des Datenzugangs für Plattformnutzer, Gewährleistung von Datenportabilität, Beschränkungen bei Kombination und Nutzung von Datenbeständen). Mit dem Ziel, die Beachtung europäischer Grundrechte und europäischer Werte bei der Nutzung Künstlicher Intelligenz durchzusetzen, bereitet die EU-Kommission derzeit weitere Gesetzgebungsinitiativen vor, die nicht zuletzt Vorgaben für Erhebung, Speicherung und Verarbeitung von Trainingsdaten für Systeme des Maschinellen Lernens enthalten sollen.

In Umsetzung europarechtlicher Vorgaben (insbesondere aus der Richtlinie (EU) 2019/770 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen) arbeitet der deutsche Gesetzgeber derzeit an der Einführung gesetzlichen Regelungen für Verbraucherverträge, die eine Bereitstellung von Daten zum Inhalt haben. Mit dem Regierungsentwurf für ein GWB-Digitalisierungsgesetz soll die Verfügungsmacht über Daten und die Zugangsmöglichkeiten zu Daten als zusätzliches Kriterium eingeführt werden, um die kartellrechtlich relevante Marktstellung eines Unternehmens zu beurteilen.

Außerdem sollen in dem Gesetz die kartellrechtlichen Voraussetzungen für einen Anspruch auf Datenzugang präzisiert werden.

Diese Beispiele zeigen, dass die Gesetzgebung im Bereich der Datenwirtschaft und der Datennutzung stark im Fluss ist. Die finale Ausgestaltung dieser neuen Vorgaben für Datenzugang und Datennutzung in der EU und in Deutschland sowie ihre Konsequenzen für die Rechts- und Vertragspraxis lassen sich derzeit noch nicht absehen.

5.6 Konsequenzen für die Praxis

Eine allgemeine Erlaubnis für die Erhebung, Sammlung, Nutzung oder Auswertung von Daten für private oder unternehmerische Zwecke ist im deutschen Recht nicht vorhanden. Andererseits ist die Erhebung, Vervielfältigung, Sammlung und Nutzung von Daten durch Unternehmen auch nicht generell verboten. Allerdings sind zum Schutz berechtigter Interessen für die Verarbeitung besonderer Datenkategorien vielfach bestimmte gesetzliche Anforderungen und Einschränkungen zu beachten.

Auch wenn ein gesetzlicher Anspruch auf Datenzugang und Datenverarbeitung nicht besteht, kann ein solcher Anspruch vertraglich begründet werden, soweit der Datenzugang vom Berechtigten eingeräumt wird und die mit dem Datenzugang verbundenen gesetzlichen Restriktionen im Vertrag berücksichtigt und tatsächlich beachtet werden.

Allerdings gelten vertraglich eingeräumte Datenzugangs- und -verwertungsrechte nicht absolut. So gibt es z. B. für zulässigerweise erhobene personenbezogene Daten gesetzliche Nutzungsbeschränkungen und Zweckbindungen. Wurden personenbezogene Daten für einen bestimmten Zweck aufgrund einer Einwilligung der betroffenen Person erhoben, so ist für eine Nutzung dieser Daten außerhalb der von der Einwilligung gedeckten Nutzung (Zweckänderung) eine weitere Erlaubnis notwendig, es sei denn, die Weiterverarbeitung ist noch vom ursprünglichen Erlaubnistatbestand gedeckt (sog. kompatible Weiterverarbeitung nach Art. 6 Abs. 4 DS-GVO).

Auch können vertragliche Rechte auf Datenzugang und Datennutzung in den Verträgen selbst begrenzt und mit Bedingungen und Auflagen versehen werden. Dadurch kann der Dateninhaber die Datennutzung durch den Vertragspartner beeinflussen und in gewisser Weise steuern. Insofern kann der Nutzwert von Daten durch Öffnung eines Datenzugangs für mehrere interessierte Unternehmen gesteigert werden, ohne dass der ursprüngliche Dateninhaber seine Datensouveränität völlig aufgeben muss.

Bitkom vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, davon gut 2.000 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org

bitkom