Leitfaden

bitkom

Datennutzung für digitale Geschäftsmodelle

Leitfaden zu Rechtsfragen und Vertragsgestaltung

Teil 2: Möglichkeiten der Vertragsgestaltung

Herausgeber

Bitkom e. V.
Albrechtstraße 10
10117 Berlin
Tel.: 030 27576-0
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner

Charleen Roloff
Referentin Legal Tech & Recht
T 030 27576-199
c.roloff@bitkom.org

Verantwortliches Bitkom-Gremium

AK Vertrags- und Rechtsgestaltung

Satz & Layout

Lea Joisten

Titelbild

Copyright

Inhalt

Vorwort und Danksagung

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

Der vorliegende zweite Teil des Leitfadens enthält Überlegungen zur Gestaltung von Verträgen über Datenzugang, Datenaustausch und Datennutzung. Dabei legt er die im ↗ ersten Teil des Leitfadens dargestellten gesetzlichen Grundlagen für Austausch und Nutzung von Daten zugrunde.

Der Leitfaden soll Denkanstöße setzen und eine erste Orientierung zu den gesetzlichen und vertraglichen Grundlagen der Datennutzung geben. Er kann aber keine endgültigen und umfassenden Lösungen präsentieren.

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 c.roloff@bitkom.org.

Diese Publikation beruht auf der spezifischen Sachkenntnis, der wertvollen praktischen Erfahrung und auf dem ehrenamtlichen Engagement von Expertinnen und 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
- Thomas Kriesel, Mazars Rechtsanwaltsgesellschaft mbH, vormals Bitkom e.V.
- Stephan Kreß, LL.M. (UC Hastings), Morrison & Foerster LLP

Berlin, Mai 2022

1 Datennutzung im Unternehmen (Wie können Unternehmen Daten nutzen?)

1.1 Möglichkeiten der unternehmerischen Datennutzung

In modernen Unternehmen fallen regelmäßig Daten und Informationen in großem Umfang und aus vielen unterschiedlichen Quellen an. Informationen werden z. B. für die Erfüllung gesetzlicher Pflichten benötigt, für die Verwaltung der Mitarbeitenden, für Buchhaltung und Besteuerung, für Marketingzwecke, zur Kontrolle und Steuerung von Unternehmensprozessen sowie zur Qualitätssicherung.

Daten ermöglichen es Unternehmen auch, ihre Geschäftsmodelle zu verfeinern und weiterzuentwickeln, ihre Prozesse effizienter zu gestalten, ihr Produkt- und Leistungsangebot zu verbessern und zu individualisieren oder ganz neue Geschäftsmodelle zu entwickeln. So reduziert z. B. die Überwachung von Maschinen und Geräten durch eine ständige Erhebung und Auswertung von Prozess- und Zustandsdaten und eine darauf gestützte frühzeitige und zielgenaue Wartung einerseits Ausfallzeiten dieser Maschinen und Geräte (Predictive Maintenance) und ermöglicht andererseits zielgenaue Produkt- und Serviceverbesserungen. Die Modellierung eines Produkts über Veränderung, Anpassung und Verbesserung von Produktionsdaten in einem virtuellen Raum beschleunigt den Konstruktionsprozess und hilft dabei, Produktions- und Transportkosten (Digital-Twin-Technology, Additive Manufacturing) zu vermeiden. Die Analyse von Daten ermöglicht es, das zukünftige Kaufverhalten und den zukünftigen Produktbedarf vorherzusagen (Predictive Analytics) und die Produkte auf die Bedürfnisse von Verbraucherinnen und Verbrauchern besser anzupassen (individualisierte Versicherungstarife, individualisierte Werbung).

Die hier nur beispielhaft genannten Verwendungsmöglichkeiten von Unternehmensdaten haben gemeinsam, dass sie auf den Datenzugang und auf die Möglichkeit, Daten zu nutzen, angewiesen sind. Soweit diese Daten aus internen Prozessen und Informationsquellen des Unternehmens stammen und auch nur intern genutzt und verarbeitet werden, sind hierfür keine besonderen Verträge notwendig. Eine Ausnahme gilt lediglich für die Verarbeitung von personenbezogenen Daten, insbesondere Daten von Arbeitnehmerinnen und Arbeitnehmern. Hierzu ist ggf. eine Betriebsvereinbarung erforderlich. Vertragliche Regelungen werden erst dann erforderlich und sinnvoll, wenn Daten mit anderen Rechtssubjekten (z. B. Kunden und Lieferanten) geteilt, ausgetauscht oder an

diese übergeben werden. Für viele solcher Geschäftsbeziehungen zum Datenaustausch und zur Datennutzung ist allerdings kein zeitlich unbegrenzter Datenzugang erforderlich. Die Nutzung der Daten kann vielmehr zweckgebunden und zeitlich begrenzt ausgestaltet werden. Dies lässt sich auch in der vertraglichen Gestaltung abbilden.

1.2 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 u. a. folgende Daten:

- Daten zur Auslastung und 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),
- Betriebs- und Servicedaten der Paletten-Shuttles (z. B. Batteriezustand, Sensor- und Kameradaten zur selbständigen Steuerung der Shuttles).

Die Daten, die das Logistikunternehmen in seinem regulären Geschäftsbetrieb erhebt und speichert, können auch für andere Unternehmen von Interesse sein, z. B. für IT-Dienstleister, weitere Dienstleister aus der Logistikbranche sowie für Marktforschungsunternehmen. Das Logistikunternehmen kann die Daten somit gewinnbringend weiterverwerten.

2 Rechtliche Vorgaben für Datenverträge

2.1 Wahl der Vertragsart für Datenverträge

Der Austausch von Daten ist nach geltendem Recht weitgehend freiwillig[1] und wird auf der Basis von Verträgen abgewickelt. Einen gesetzlichen Zwang für Privatrechtssubjekte, Daten miteinander auszutauschen, kennt das Gesetz nur in Ausnahmefällen unter besonderen Voraussetzungen (z. B. bei einer dominierenden Marktstellung des Dateninhabers).

Die möglichen Regelungen des Verordnungsvorschlags der EU-Kommission zum Data Act vom 23. Februar 2022 wurden in diesem Leitfaden noch nicht berücksichtigt. Geplant sind unter anderem Datenzugangsansprüche auf Daten, welche im Kontext der Nutzung von IoT-Geräten und -Diensten anfallen. Wir gehen davon aus, dass der Data Act und weitere (sektorale) regulatorische Vorhaben mittelfristig signifikante Änderungen in Recht und Vertragsgestaltung mit sich bringen werden, welche gerade im datenwirtschaftlichen Kontext rechtliche, strategische und operative Auswirkungen haben können. Wir gehen in diesem Leitfaden jedoch nicht weiter darauf ein, weil das Gesetzgebungsverfahren noch andauert und die Regelungen deshalb noch ungewiss sind.

Leistung und Gegenleistung für eine (dauerhafte) Datenübertragung können vielfältiger Natur sein, insbesondere kann die Gegenleistung für eine Datenübertragung ganz oder teilweise in einer Vergütung (Geldzahlung), in der Bereitstellung anderer Daten (wechselseitige Datenlieferung), in der Nutzung eines Gegenstandes oder einer Infrastruktur (z. B. Gewährung des Zugangs zu einem Netzwerk) oder in der Nutzung eines bestimmten Dienstes (z. B. Zugriffsrecht auf bestimmte Datenauswertungsergebnisse einer bestimmten Datenanalyse) bestehen.

Abhängig vom konkreten Modell der Datenbereitstellung ist die Einordnung in einen bestimmten Vertragstyp vorzunehmen. Das deutsche Recht stellt die allgemeinen Vertragstypen Dienstvertrag (§ 611 BGB), Kaufvertrag (§ 433 BGB), Mietvertrag (§ 535 BGB), Pachtvertrag (§ 581 BGB), Leihe (§ 598 BGB), Werkvertrag (§ 631 BGB), Tauschvertrag (§ 480 i. V. m. § 433 BGB) und Schenkung (§ 516 BGB) zur Verfügung. Es gibt ergänzende Vorschriften für Verbraucherverträge, bei denen der Verbraucher dem Unternehmer personenbezogene Daten bereitstellt oder sich dazu verpflichtet (§ 312 Abs. 1a BGB) sowie für Verträge über digitale Produkte (§§ 327 ff. BGB). Jedoch kennt das BGB keinen speziell auf Datenaustausch und Datennutzung ausgerichteten Vertragstyp.

1 Die Förderung eines freiwilligen Datenaustausches ist ein wesentliches Ziel in der Datenstrategie der Bundesregierung, vgl. Kabinettsfassung der ↗ Datenstrategie der Bundesregierung vom 27. Januar 2021, S. 22.

Daher sind in Datenverträgen Regelungen zu vereinbaren, die die gesetzlichen Regelungsfolgen abändern und ergänzen. Entsprechende Vereinbarungen unterliegen jedoch gesetzlichen Einschränkungen, die im Folgenden kurz skizziert werden. Die Datenbereitstellung kann aber auch als Nebenleistung eines Vertrages ausgestaltet sein – etwa, um die eigentlichen vertragsgegenständlichen Leistungen erbringen zu können oder zu verbessern.[2]

2.2 Vorgaben des AGB-Rechts

Nach den für Allgemeine Geschäftsbedingungen (AGB) einschlägigen Vorschriften (§§ 305 ff. BGB) sind wesentliche Abweichungen vom Leitbild eines gesetzlich geregelten Vertragstyps durch einseitige Formulierungsvorgaben einer Vertragspartei unzulässig, wenn sie die andere Vertragspartei unangemessen benachteiligen (vgl. Wertung des § 307 BGB). Da das deutsche Recht spezielle Leitbilder für Datenverträge nicht kennt, ist die Wirksamkeit von AGB für solche Verträge mit gewissen Unsicherheiten verbunden. Mit den Vorgaben des AGB-Rechts wäre aber z. B. der vollständige Ausschluss von Haftungsansprüchen des Datenanbieters für Rechtsgutsverletzungen oder für Sach- und Rechtsmängel nicht vereinbar, da dies unbestreitbar mit den wesentlichen Grundgedanken der gesetzlichen Vertragstypen nicht zu vereinbaren wäre. Da Muster- und Standardverträge regelmäßig als AGB anzusehen sind, sind für ihre Gestaltung die AGB-Inhaltskontrolle (§§ 307, 308 Nr. 3 BGB) und das Verbot überraschender Klauseln (§ 305c BGB) zu beachten.[3]

2 So könnten z. B. KI-Anbieter ein Interesse daran haben, Einblicke in die von Kunden mit einer KI-Software verarbeiteten Daten zu erhalten, um die Software und ihre Algorithmen weiterzuentwickeln.

3 Vor diesem Hintergrund wäre eine AGB-Klausel, wie sie in dem folgenden Beispiel verwendet wird, unwirksam, da sie sowohl gegen das Verbot überraschender Klauseln als auch gegen das Gebot von Treu und Glauben verstieße. Beispiel: Im Rahmen der Einführung eines Software-Tools in der Finanzabteilung eines Unternehmens behält sich der Software-Anbieter in seinen Lizenzbedingungen vor, dass alle Daten und Informationen, die durch das Tool erfasst und dadurch im weitesten Sinne verarbeitet werden, exklusiv dem Software-Anbieter zustehen.

2.3 Vorgaben des geistigen Eigentums

Bestimmte Einzeldaten oder Daten(teil)mengen können spezifischen Schutzgesetzen unterliegen (etwa Urheberrechtsgesetz, Patentgesetz, Geschäftsgeheimnisgesetz). In diesem Fall können zusätzliche Anpassungen und Ergänzungen bei der Vertragsgestaltung veranlasst sein. Denn neben der Einräumung eines tatsächlichen Datenzugriffs ist in diesen Fällen immer auch eine Nutzungserlaubnis einzuräumen, die vom Schutzrechtsinhabenden abgeleitet werden kann. Für Daten, die keinem spezifischen Schutzrecht unterliegen, sind häufig nur schuldrechtliche Vereinbarungen für die Nutzung zwischen den Vertragspartnern möglich, die jedoch keine Wirkung gegenüber Dritten entfalten.

2.4 Besonderheiten für einzelne Datenkategorien

Gesetzliche Vorgaben für den Austausch von Daten und für die hierfür abzuschließenden Datenverträge bestehen nur ausnahmsweise für bestimmte Datenkategorien (z. B. für Smart Grid-Daten, Zahlungsdaten oder sonstige personenbezogene Daten z. B. im Hinblick auf Datenportabilität). Die gesetzlichen Vorgaben sind im Vertrag zu berücksichtigen.

Besondere Anforderungen gelten bei der Einräumung von Nutzungsmöglichkeiten und dem Datenzugang für Daten, auf die sich ein Recht des geistigen Eigentums erstreckt. Bei solchen Daten reicht die reine Gewährung des Datenzugangs nicht aus und ein zusätzliches Nutzungsrecht muss als »Ausschnitt« des Schutzrechts übertragen werden.

3 Eckpunkte für Datenverträge (Was ist vor Vertragsschluss wichtig?)

3.1 Notwendige Vorfestlegungen

Inhalt und Ausgestaltung eines Datenvertrages werden maßgeblich durch Entscheidungen bestimmt, die vor Vertragsabschluss getroffen werden müssen. Denn Verträge über Daten sind vielfältig. Von tätigkeitsbezogenen Datenauswertungsverträgen über eine befristete Datenüberlassung bis hin zu einer Datenüberlassung auf Dauer (Datenkauf) sind zahlreiche Gestaltungen denkbar. Zusammen mit der Datenüberlassung können Datennutzungs- und Datenzugriffsbeschränkungen in den Grenzen der geltenden Gesetze vereinbart werden. Auch ist eine gemeinsame und kooperative Datennutzung durch mehrere Akteure denkbar.

Mindestens über folgende relevante Umstände sollte vor Abschluss eines Datenvertrages Klarheit bestehen:

- Identifizierung und Abgrenzung der vertragsgegenständlichen Datenbestände (welche Daten, welche Datenquellen, wie produziert, bei wem gespeichert, mit welchem Informationsgehalt, personenbezogen oder nicht-personenbezogen?)
- Identifizierung von möglicherweise bestehenden Schutzrechten an den vertragsgegenständlichen Daten (z. B. Urheberrechte, Geschäftsgeheimnisschutz, Datenschutz). Besteht ein solches Schutzrecht, ist dem Datennutzer neben dem Datenzugang ein Nutzungsrecht am vertragsgegenständlichen Datenbestand einzuräumen. Außerdem sollten ggf. Beschränkungen dieses Nutzungsrechts im Vertrag vereinbart werden.
- Festlegung von Zweck, Umfang und Grenzen für die Datennutzung und entsprechend für den Datenvertrag (was soll mit dem Vertrag erreicht werden?)
- Identifizierung der Rollen der Vertragspartner: Datenlieferant, Datennutzer, Plattformbetreiber zur Gewährung / Vereinfachung / Verwaltung des Datenzugriffs
- Zuweisung der Dateninhaberschaft: Dies dient der Rechtssicherheit und empfiehlt sich insbesondere bei unklarer Ausgangslage mit mehreren potenziellen Dateninhabern. Fehlt eine explizite Regelung, wären die Daten demjenigen zuzuordnen, der den wirtschaftlich-organisatorischen Aufwand für die Erzeugung eines Datenbestandes trägt.[4]

4 Digitalisierte Wirtschaft / Industrie 4.0, Gutachten im Auftrag des BDI (2015), S. 25.

- Art und Weise des Datenzugangs einschließlich Identifizierung technischer Schnittstellen bzw. von Technologien und Verantwortlichkeiten zur Datenübertragung und Datenformaten
- Identifizierung von möglichen Fehlerquellen: z. B. IT-Sicherheitslücken, fehlerhafte Übertragung, unzureichende Datenqualität, nicht ausreichende Anonymisierung
- Gegenleistung für die Datenbereitstellung.

3.2 Formen des Datenzugangs

In der aktuellen Diskussion werden gern Begriffe wie Datenzugang, Datenzugriff oder Datenaustausch (Data-Exchange) verwendet. Diese Begriffe sind jedoch für die Vertragsgestaltung zu vage und müssen daher konkretisiert werden. Ein Datenzugang kann unterschiedliche konkrete Ausformungen annehmen, die voneinander abzugrenzen sind. Die im Folgenden definierten Formen des Datenzugangs grenzen rein tatsächliche Zugangsmöglichkeiten zu Daten ab. Die beschriebenen Formen des Datenzugangs sind nicht mit Rechten zur Datennutzung identisch, sondern folgen aus dem jeweils vertraglich vereinbarten Recht zur Datennutzung.

- Die Herausgabe von Daten ist durch die Rechtsprechung definiert als die Übermittlung eines Datenbestandes an einen anderen Rechtsträger und die Löschung der Daten in der eigenen Sphäre des Herausgabeverpflichteten.[5] Der Herausgabeverpflichtete bleibt also seinerseits nicht Dateninhaber. Eine Datenherausgabe kommt insbesondere bei Beendigung einer Vertragsbeziehung in Betracht.
- Wird ein einseitiger Datenzugang für eine Vertragspartei eröffnet und hat der bisherige Dateninhaber noch immer Zugriff auf den Datenbestand, könnte man von Datenbereitstellung sprechen. Eine Datenbereitstellung auf Dauer (Datenübertragung) gegen Entgelt wäre über einen Kaufvertrag abzuwickeln, eine befristete Datenbereitstellung (Datenüberlassung) über einen Miet- oder Pachtvertrag. Je nach vertraglicher Vereinbarung kann die Datenbereitstellung eine aktive Übermittlung eines Datenbestandes in die Sphäre des Vertragspartners erfordern oder in der bloßen Datenbereitstellung für einen Zugriff durch den Vertragspartner bestehen. Zu unterscheiden ist auch, ob eine Datenbereitstellung zur freien Verfügung des Vertragspartners erfolgt (inklusive den Befugnissen zur Bearbeitung und Ergänzung mit anderen Daten, zur Analyse, zur kommerziellen Verwendung und Weitergabe an Dritte) oder ob die Nutzung des bereitgestellten Datenbestandes auf eine interne Nutzung durch den Vertragspartner beschränkt ist. Ein Datenzugriff zur Informationsvermittlung, der auf einen Lesezugriff ohne die Möglichkeit und Befugnis zum Kopieren, d. h. auf die bloße Kenntnisnahme der bereitgestellten Informationen, beschränkt ist, könnte als Dateneinsicht bezeichnet werden.

5 BGH, Urteil vom 17.04.1996, Az. VIII ZR 5/95.

- Ist die Befugnis zur Einsichtnahme in einen Datenbestand mit einer Möglichkeit und einer Befugnis zum Kopieren einzelner Datensätze oder des gesamten zugänglichen Datenbestandes verbunden, könnte von Datenauslesen gesprochen werden. Ein solches Auslesen der Daten könnte z. B. an definierten Mess- oder Sensorpunkten in der Sphäre des Vertragspartners stattfinden.
- Ein Analysezugriff liegt vor, wenn ein Datenzugang mit dem Zugriff auf die Ergebnisse einer Datenauswertung verbunden ist. Der Analysezugriff kann auf die Ergebnisse einer Datenanalyse durch den Vertragspartner beschränkt sein, die Befugnis zur Nutzung eigener Analysetools für den Datenpool des Vertragspartners oder die Nutzung von Analysetools des Vertragspartners umfassen.
- Data Mining ist die Nutzung großer Datenmengen, die vom Data Miner analysiert werden, um Muster, Strukturen oder Zusammenhänge aufzudecken. Neben der Regelung des Datenzugangs für den Data Miner ist auch der Inhalt des Nutzungsrechts zu bestimmen. Dabei stellt der Data Miner seine Auswertungsergebnisse häufig dem Datenberechtigten zur Verfügung.
- Datenaustausch (Data-Exchange) ist die gegenseitige Gewährung eines Datenzugriffs auf jeweils in der Sphäre der Vertragspartner befindliche Datenbestände.
- Datenpooling ist die Nutzung eines von den Vertragsparteien gemeinsam aufgebauten Datenbestandes. Neben Umfang und Reichweite der Nutzungsrechte und den Verpflichtungen zur Vergrößerung des Datenpools sind in solchen Konstellationen insbesondere vertragliche Bestimmungen dazu erforderlich, wie der Datenpool bei Vertragsende auf die Vertragsparteien aufgeteilt wird.

4 Regelungsinhalte für Datenkaufverträge

In diesem Kapitel werden mögliche Grundmodule für Verträge über die dauerhafte Überlassung von Daten gegen Vergütung (Datenkauf) vorgestellt.[6] Dabei ist die Datenbereitstellung als Hauptleistungspflicht ausgestaltet.[7] Wesen des Kaufs ist, dass der Käufer eine zeitlich unbeschränkte Verfügungsmöglichkeit über den Vertragsgegenstand erhält. Der Käufer ist also bei planmäßiger Vertragsdurchführung nicht zur Rückgabe oder zur Löschung der vertragsgegenständlichen Daten verpflichtet.

Die im Einzelfall zu vereinbarenden Vertragsinhalte können so komplex, vielschichtig, speziell und umfangreich sein, dass sie sich nicht in allgemeinen Vertragsregelungen abbilden lassen. Dementsprechend können Verträge weitergehende Regelungen zu Nutzungsrechten an Daten (z. B. Bedingungen für die Weiterverteilung der Daten) bis hin zu Auditrechten des Datenlieferanten enthalten, die hier nicht erörtert werden. Die folgenden Abschnitte sollen jedoch eine Orientierung geben, welche Regelungen und Bedingungen der Datennutzung sinnvoll und angemessen sein könnten. Dabei sind sie auf eine B2B-Geschäftsbeziehung zwischen zwei Vertragspartnern ausgerichtet.

4.1 Vertragszweck

a) Einführung

Es ist zu empfehlen, in einer allgemeinen vertraglichen Regelung (z. B. in einer Präambel) den Zweck des jeweiligen Datenvertrages festzulegen. Dies ist nicht zuletzt deswegen von Bedeutung, weil die übrigen Regelungen des Vertrages im Licht des Vertragszwecks ausgelegt und auf diese Weise etwaige Lücken der vertraglichen Absprachen im Nachhinein gefüllt werden (jedenfalls bei Aufnahme einer entsprechenden Auslegungsklausel in den Vertrag). Daher sollte im Vertrag explizit niedergelegt sein, wozu der Käufer die überlassenen Daten benötigt und wofür er sie verarbeitet, für welche Verarbeitung die vertragsgegenständlichen Daten nicht geeignet sind (zur Begrenzung des Umfangs für Haftung und Gewährleistung), ob der Käufer die erhaltenen Daten kommerziell nutzen (insbesondere weiterverkaufen) darf und ob der Verkäufer an den

6 Sollen die Daten im Rahmen einer Schenkung und damit ohne Gegenleistung des Empfängers übertragen werden, empfiehlt sich aus Beweisgründen auch die Vereinbarung darüber, dass keine Gegenleistung geschuldet ist, explizit in den Vertrag aufzunehmen. Bei der schenkungsweisen Überlassung gelten gesetzliche und vertragliche Besonderheiten, auf die nachfolgend nicht weiter eingegangen werden soll.

7 In der Praxis sind auch Konstellationen anzutreffen, in denen die Bereitstellung der Daten eine Nebenleistungspflicht darstellt oder Daten lediglich beigestellt werden, um die Erfüllung anderer vertraglicher Pflichten zu ermöglichen (z. B. Bereitstellung von Testdaten in einem Softwareprojekt). Die Darstellung dieser Konstellationen würde jedoch den Rahmen dieses Leitfadens sprengen.

Vorteilen aus der Weiternutzung beteiligt werden soll. Wird mit der Datenübertragung ein gleichgerichtetes Ziel beider Vertragsparteien verfolgt, sollte auch dies im Vertrag niedergelegt werden.

Schließlich grenzt der Vertragszweck im Zusammenspiel mit weiteren vertraglichen Regelungen die zulässige Datennutzung der Parteien ein. Zum Schutz des Verkäufers kann an eine vertragszweckwidrige Datennutzung ein Sonderkündigungsrecht oder eine Vertragsstrafe geknüpft werden.

b) Formulierungsvorschlag (in Anlehnung an das Betrachtungsbeispiel unter ↗ Ziffer 1.2)

Vertragszweck: Zweck dieses Vertrages ist die Überlassung von Betriebs- und Servicedaten der beim Logistikunternehmen L in Einsatz befindlichen elektrischen Paletten-Shuttles. Die Daten werden dem Hersteller der Shuttles zur Verfügung gestellt, damit dieser Funktionalität, Robustheit und Wartung der Shuttles verbessern kann und seinen Kunden zukünftig entsprechend optimierte Produkte und Wartungsleistungen anbieten kann.

4.2 Leistungsbeschreibung

a) Einführung

In der Leistungsbeschreibung legen die Vertragsparteien fest, welche Daten oder Datensätze zwischen ihnen übertragen und in welcher Form diese Daten bereitgestellt werden müssen. Dabei sollten die Vertragsparteien auch prüfen, ob die Daten vom Wirkungsbereich eines gesetzlichen Rechts zum Schutz des geistigen Eigentums erfasst werden. In diesem Fall müsste ein besonderes Nutzungsrecht an den Daten eingeräumt werden (↗ vgl. unten Ziffer 4.3). Die Leistungsbeschreibung sollte so detailliert und eindeutig wie möglich sein. Denn eine genaue und detaillierte Leistungsbeschreibung erleichtert die Vertragsdurchführung. Außerdem gehört die Leistungsbeschreibung zu den wesentlichen Vertragsbestandteilen (essentialia negotii), die frei von den Vorgaben und Wertungen des AGB-Rechts vereinbart werden können. So könnte z. B. durch Beschränkung einer Bereitstellungpflicht für Daten aus einer konkret bezeichneten Maschine verhindert werden, dass der Verkäufer andere Dateninhalte oder eine andere Datenqualität schuldet als durch die Maschine erzeugt werden (§ 434 Abs. 5 BGB). Nicht zuletzt bestimmen sich nach den vertraglich festgelegten Leistungspflichten der Vertragspartner der gesetzliche Vertragstyp und damit die einschlägigen gesetzlichen Vorgaben für den Vertrag. Besteht z. B. die Leistung darin, die Ergebnisse aus der Analyse eines vorhandenen Datenbestands bereit zu stellen, ist ein vertraglicher Erfolg geschuldet und somit Werkvertragsrecht anwendbar. Der hier betrachtete Vertrag über die Bereitstellung von Daten zur unbefristeten Nutzung

unterliegt dem Kaufrecht (§ 433 BGB). In die Leistungsbeschreibung können mögliche Nebenleistungen (z. B. die Mitlieferung von Analysetools) aufgenommen werden.

b) Beschreibung der vertragsgegenständlichen Daten

Die Beschreibung der Daten, die dem Vertragspartner zur Verfügung zu stellen sind, kann z. B. anhand der folgenden (nicht abschließend aufgezählten) Parameter erfolgen:

- Art der Daten (z.B. Rohdaten, Maschinen-, Umwelt-, Prozess-, Produktdaten, Marktinformationen)
- Informationsgehalt der Daten (Beschreibung, welche Sachverhalte in den Daten abgebildet werden, z. B. Daten über Bewegungsprofile oder Kundenverhalten)
- Datenquelle bzw. Bezugsobjekt der Daten
- Bestehender Personenbezug bzw. Bezugssubjekt der Daten
- Bestehende Schutzrechte an den Daten (z. B. Urheber- oder Datenbankrechte, Geheimnisschutz)
- Datenformat (z.B. .doc, .xml, Excel, maschinenlesbar und/oder menschenlesbar, über Blockchain zu übermitteln, beim Käufer unproblematisch weiter verarbeitbar)
- Datensatzbeschreibung (mit Bezeichnung der jeweiligen Datenfelder)
- Anzahl der Datensätze
- Herkunft der Daten (von Dritten erworben, selbst erstellt, noch zu erstellen)
- Datenqualität
- Datenaktualität (Zeitpunkt bzw. Zeitraum der Datenerhebung)
- Speicherort der Daten bzw. Bezeichnung des Datenträgers
- Prozess, Methode und / oder Technik der Datengewinnung, falls die vertragsgegenständlichen Daten noch erzeugt werden müssen
- anhand einer Spezifikation des Vertragspartners, die dieser nach Einsichtnahme in den zur Verfügung stehenden Datenpool erstellt.

Bei der Bestimmung der vertragsgegenständlichen Daten können auch verschiedene der genannten Parameter kombiniert werden. Es müssen aber nicht sämtliche Parameter zur Datenbeschreibung zwingend genutzt werden. Die Beschreibung und die Abgrenzung der vertragsgegenständlichen Daten werden in der Praxis vielfach auch in eine Anlage zum Vertrag ausgegliedert.

c) Bereitstellungsform der vertragsgegenständlichen Daten

Zur Leistungsbeschreibung eines Datenvertrages gehört des Weiteren die Festlegung, in welcher Form der Datenzugang eröffnet werden soll (↗ vgl. Ziffer 3.2 zu den grundsätzlich möglichen Formen des Datenzugangs). Dabei sollten – wenn nicht bereits im Rahmen des Vertragszwecks festgelegt – Zweck, Art und Dauer des Datenzugriffs präzisiert werden. Die Daten können dem Käufer z. B. durch Übergabe eines Datenträgers mit den vertragsgegenständlichen Daten, durch Datenbereitstellung in der Cloud oder auf einem Server samt Eröffnung einer Datenabrufmöglichkeit für den Käufer oder durch Einräumung eines Datenzugriffs direkt auf die Quelle der Datenerzeugung zugänglich gemacht werden. Sollen die Daten über das Internet oder in der Cloud verfügbar gemacht werden, bietet sich an, die Daten zu verschlüsseln, sodass sie nur für den Käufer zugänglich und nutzbar sind.

Die vereinbarte Bereitstellungsform entscheidet auch darüber, welche Voraussetzungen die Vertragsparteien für die Datenbereitstellung schaffen müssen und wann der Gefahrübergang an den vertragsgegenständlichen Daten stattfindet – wann also der Verkäufer seine Leistungspflicht erfüllt hat und den Kaufpreis verlangen kann. Ist z. B. ein Filehosting vereinbart, hat der Verkäufer die Daten auf einem für den Käufer zugänglichen Speicher abzulegen und dem Käufer die für den Zugang notwendigen Informationen (z. B. Passwort oder Entschlüsselungsalgorithmus, falls Daten verschlüsselt bereitgestellt werden) mitzuteilen. Ist für den Zugang zu den Daten, für deren Auslesen oder für deren Verarbeitung eine besondere Client-Software erforderlich, sind die Rechte an der Nutzung dieser Software mit zu übertragen.

Der Verkäufer sollte sich darüber im Klaren sein, dass sein Vertragspartner aus den übermittelten Daten ggf. Rückschlüsse auf seine betrieblichen Verhältnisse ziehen kann. Aus den im Beispiel unter ↗ Ziffer 1.2 übermittelten Servicedaten für die Paletten-Shuttles lassen sich z. B. Rückschlüsse auf die Auslastung der Shuttles und damit auf die aktuelle Geschäftssituation des Logistikunternehmens ziehen. Sind solche Rückschlüsse möglich, aber nicht gewollt, sollten eine entsprechende Vertraulichkeitsregelung oder ein Verbot der Datenauswertung für solche außervertraglichen Zwecke vereinbart werden (↗ vgl. dazu unten Ziffer 4.4).

d) Formulierungsvorschlag (in Anlehnung an das Betrachtungsbeispiel unter ↗ Ziffer 1.2)

Gegenstand dieses Vertrages ist die Übertragung der in diesem Vertrag (bzw. in der Anlage XY) näher bezeichneten Daten bzw. Datensätze zur unbefristeten Verfügung gegen eine einmalige Vergütung. Schutzrechte des geistigen Eigentums sind für die nach diesem Vertrag übertragenen Daten nicht einschlägig.

Der Verkäufer gewährt dem Käufer über einen Zeitraum von drei Monaten den Zugang zu folgenden Betriebsdaten zu den im Betrieb des Datenbereitstellers eingesetzten Paletten-Shuttles:

- Stromverbrauch
- Batterielaufzeit
- Ausfallzeiten wegen Batterieladung
- Länge der zurückgelegten Fahrstrecke
- Anzahl der durchgeführten Fahrten
- Gewicht der beförderten Güter
- Anzahl und Dauer von Systemstörungen, Anzahl und Härte von Kollisionen mit der Umgebung (über Sensordatenauswertung)
- Reifenabnutzung.

Der Verkäufer stellt die vertragsgegenständlichen Daten unter der folgenden Internetadresse _____ zum Download bereit. (Alternativ: Der Datenbereitsteller übermittelt die vertragsgegenständlichen Daten auf einem maschinenlesbaren Datenträger. Alternativ: Der Verkäufer eröffnet für den Käufer über die folgende Schnittstelle _____ eine Zugriffsmöglichkeit auf den vertragsgegenständlichen Datenbestand.)

4.3 Rechteeinräumung

a) Einführung

Wesen des Datenkaufs ist der Übergang der vertragsgegenständlichen Daten in den Verfügungsbereich des Käufers und die Einräumung einer zeitlich unbefristeten Möglichkeit zur Nutzung der Daten. Anders als für Sachen kommt für Daten eine Eigentumsübertragung nicht in Betracht, da das deutsche Recht ein Eigentum an Daten nicht anerkennt. Daher hat der Verkäufer mit der Übertragung des vertragsgegenständlichen Datenbestandes bzw. mit der Einräumung einer Zugriffsmöglichkeit auf den vertragsgegenständlichen Datenbestand für den Käufer seine wesentliche Vertragspflicht bereits erfüllt. Ein explizites Nutzungsrecht für die Nutzung der vertragsgegenständlichen Daten muss der Verkäufer zusätzlich nur einräumen, wenn die vertragsgegenständlichen Daten von einem besonderen Schutzrecht (z. B. Urheberrecht, Designrecht, Patentrecht, Datenbankherstellerrecht) erfasst werden. Dann ist eine »echte Lizenzierung«, d. h. die Übertragung eines Nutzungsrechts als Ausschnitt des einschlägigen Schutzrechts erforderlich. Dabei sollten die Schutzrechte, die im Zusammenhang mit den vertragsgegenständlichen Daten bestehen sowie deren Umfang und Reichweite genau beschrieben werden.

Im Rahmen der Rechteeinräumung sollte auch geklärt werden, ob der Verkäufer ein eigenes Nutzungsrecht an den Daten behalten soll oder nicht. Im ersten Fall wäre nur ein einfaches Nutzungsrecht an den Käufer zu übertragen. Insgesamt sollten an den

vertragsgegenständlichen Daten keine Rechte von Personen bestehen, die nicht Vertragspartei sind und nicht in die Datenübertragung eingewilligt haben. Ansonsten könnte der Verkäufer einer Rechtsmängelhaftung unterliegen. Ist die Datenübertragung darauf ausgerichtet, dass der Käufer ein bestimmtes Datenverarbeitungsergebnis erzielt (z. B. Anlernen einer KI), sollte auch geklärt werden, wem dieses Datenverarbeitungsergebnis zuzuordnen ist und ob der Verkäufer daran ggf. Rechte erwerben soll.

b) Formulierungsvorschlag (in Anlehnung an das Betrachtungsbeispiel unter ↗ Ziffer 1.2)

Der Verkäufer überträgt den vertragsgegenständlichen Betriebsdaten der Paletten-Shuttles frei von eigenen Schutzrechten und von Rechten Dritter. Der Käufer erhält ein nicht-ausschließliches, zeitlich und räumlich unbeschränktes Recht zur Verarbeitung der vertragsgegenständlichen Daten. Der Käufer ist insbesondere befugt, die vertragsgegenständlichen Daten mit anderen Datenbeständen zu ergänzen und zu vermischen, die übertragenen Daten ganz oder teilweise zu löschen und Auswertungen der vertragsgegenständlichen Daten vorzunehmen sowie die vertragsgegenständlichen Daten in anderer Weise zu bearbeiten und eigene Schutzrechte an dem übertragenen Datenbestand zu begründen.

4.4 Nutzungsbedingungen und –auflagen

a) Einführung

Für den Verkäufer kann es sinnvoll sein, an die Nutzung der übertragenen Daten bestimmte Auflagen und Bedingungen zu knüpfen oder die Nutzung einzuschränken. Solange hinter diesen Einschränkungen berechtigte Interessen des Verkäufers stehen, dürften sie auch mit den Vorgaben des AGB-Rechts vereinbar sein. So lässt sich z. B. ein Geschäftsgeheimnisschutz an den übermittelten Daten nur aufrechterhalten, wenn der Verkäufer als Geschäftsgeheimnisinhaber dem Käufer angemessene Schutzmaßnahmen auferlegt. Auch lässt sich ein Verbot der Weiterübertragung der Daten an Dritte, vor allem an Wettbewerber des Verkäufers, durchaus rechtfertigen. Da Nutzungsbeschränkungen nur schuldrechtlicher Natur sind, wirken sie nur gegenüber dem Vertragspartner und nicht gegenüber am Vertrag nicht beteiligten Dritten. Gibt der Vertragspartner die Daten ohne Zustimmung des Verkäufers an einen gutgläubigen Dritten weiter, hat der Verkäufer gegen den Dritten keinen Anspruch auf Herausgabe der Daten.[8] Daher sollte er versuchen, Sanktionsmaßnahmen für den Fall einer unbefugten Datenweitergabe durch den Käufer im Vertrag zu etablieren.

8 Da Daten für sich genommen keine körperlichen Sachen im Sinne des § 90 BGB sind, sind die Besitzschutzvorschriften des BGB (§§ 854 ff. BGB) auf sie nicht anwendbar.

Weitere ggf. regelungsbedürftige Punkte:

- Kontrollbefugnisse des Datenbereitstellers (Auditrechte) zur Überprüfung, ob die Nutzungsbedingungen und –auflagen eingehalten wurden
- Konsequenzen für einen Verstoß gegen Nutzungsbedingungen: Vertragsstrafen, Rücktritt
- Umfang der Datennutzung: Einmalige / mehrmalige / unbegrenzte Datennutzung; Unterlassung weitergehender Nutzung
- Geographische Beschränkung der Datennutzung, Unterlassung der Nutzung oder des Zugriffs außerhalb des Nutzungsraums
- Verwendung der Nutzungsergebnisse: Der Umfang, in welchem die Ergebnisse der Datennutzung selbst genutzt werden können; Unterlassung weitergehender Nutzung von Ergebnissen
- Ausschließlichkeit der Datennutzung: Nicht- / Ausschließlichkeit der Datennutzung (ggf. mit Einschränkungen)
- Sicherung der Einhaltung von Rechten zur Datennutzung: Auskunftspflichten und Kontrollrechte für Datennutzung; technische Schutzmaßnahmen gegen nicht vereinbarte Datennutzung (zwecks Geschäftsgeheimnisschutz)

b) Formulierungsvorschlag (in Anlehnung an das Betrachtungsbeispiel unter ↗ Ziffer 1.2)

Der Käufer darf die Daten zur Erreichung der sich aus diesem Vertrag ergebenden Nutzungszwecke verarbeiten. Eine Nutzung der Daten für andere Zwecke durch den Käufer ist nicht gestattet. Dem Käufer ist eine Auswertung der Daten untersagt, soweit die Auswertung darauf gerichtet ist, Erkenntnisse auf Betriebsabläufe und Geschäftstätigkeit des Verkäufers zu gewinnen. Erhält der Käufer auf anderem Weg Kenntnis von Betriebsabläufen und Geschäftstätigkeit des Verkäufers, ist ihm die Weitergabe dieser Informationen untersagt. Der Käufer ist nicht berechtigt, die vertragsgegenständlichen Daten oder Erkenntnisse aus deren Auswertung an Dritte zu übertragen oder Dritten auf andere Weise Zugriff auf die vertragsgegenständlichen Daten zu gewähren.

4.5 Gegenleistung

Die Leistungspflicht liegt bei einem Datenkauf in der einmaligen Überlassung von Daten bzw. digitalen Inhalten, die Gegenleistung ist die Zahlung eines Entgelts. Bei dem zugrunde liegenden Vertragsverhältnis handelt es sich in der Regel um einen Kaufvertrag über sonstige Gegenstände. Es gelten dementsprechend die Vorschriften zum Kaufvertrag mit den entsprechenden Gewährleistungsansprüchen (↗ vgl. unten Ziffer 4.6). Es kann sich aber auch um einen Werklieferungsvertrag gemäß § 650 BGB handeln, z. B. dann, wenn die einmalig bereitgestellten Daten erst noch erzeugt werden (müssen). Nach § 650 Abs. 1 S. 1 BGB kommen dann ebenfalls die Vorschriften des Kaufvertragsrechts zur Anwendung. Auch im Falle des Datentauschs, bei dem nicht das Entgelt die Gegenleistung ist, sondern die Bereitstellung anderer Daten, finden nach § 480 BGB die kaufvertragsrechtlichen Regelungen Anwendung.

Beim Datenkauf stellen sich insbesondere schuldrechtliche Fragen, wie z. B. die Ausgestaltung der Leistungspflicht und die Folgen einer Leistungsstörung.

Je nachdem, ob es sich um personenbezogene oder lediglich um Maschinen-Daten handelt, sind die datenschutzrechtlichen Besonderheiten und Vorschriften zu beachten. Die Leistungspflicht in einem schuldrechtlichen Vertrag zur Übermittlung von personenbezogenen Daten muss dabei, soweit erforderlich, die (widerrufliche) datenschutzrechtliche Einwilligung zur Nutzung der Daten umfassen.

Gleichzeitig kann, je nach dem Wert der Daten, der Schutz der Daten als Leistungsgegenstand vertraglich über die Anwendung des Geschäftsgeheimnisschutzgesetzes erweitert und die Verbreitung der Daten beschränkt werden.

Im Rahmen der Leistungsstörung finden die §§ 280, 281, 275, 320 ff. und 323 BGB grundsätzlich Anwendung. Eine Pflichtverletzung des Datenschuldners kann beim Datenkauf in dem Zurverfügungstellen von falschen Daten liegen. Dies kann schlicht als Nichtleistung und damit als Verletzung der vertraglichen Pflicht gewertet werden. Die Beweisführung über den Schaden und die Bezifferung des Schadens dürfte hingegen schwerlich möglich sein.

Die Richtlinie über bestimmte vertragliche Aspekte der Bereitstellung digitaler Inhalte (EU 2019/770, i.F. »DI-RL«), die bis zum 01.07.2021 umzusetzen war und seit dem 01.01.2022 in Deutschland mit der Änderung des Bürgerlichen Gesetzbuches, u. a. in den §§ 312 ff. und den §§ 327 ff. BGB, umgesetzt wurde, erstreckt sich auf Verträge zwischen Unternehmern und Verbrauchern, die die Bereitstellung digitaler Inhalte oder digitaler Dienstleistungen zum Gegenstand haben. Sie bezieht sich also auch auf den oben beschriebenen Datenkaufvertrag, bei dem z. B. die Leistung des Unternehmers darin liegen kann, Daten bereitzustellen, für die der Verbraucher ein Entgelt leistet.

Die vermeintliche Beschränkung des Anwendungsbereichs der DI-RL auf das B2C-Verhältnis schlägt tatsächlich auch auf den B2B-Bereich durch. Denn die neuen Leistungspflichten im Verbrauchergeschäft haben ihre Ausstrahlungswirkung auf die gesamte Lieferkette und müssen damit de facto beim Hersteller ansetzen. Auch die für das Verbrauchergeschäft zwingenden Regressvorschriften gilt es in der Lieferkette zu berücksichtigen (siehe auch § 327u BGB). Der Anwendungsbereich ist damit nicht auf den Verbrauchervertrag beschränkt, sondern muss auch darüber hinaus berücksichtigt werden.

4.6 Gewährleistung

a) Einführung

Insbesondere die Qualität der Daten spielt für ihre Nutzbarkeit und damit im Rahmen der Mängelgewährleistung eine entscheidende Rolle. Der Kauf von Daten stellt sich als Kauf von »sonstigen Gegenständen« dar, auf den gemäß § 453 Abs. 1 Var. 2 BGB das Kaufvertragsrecht entsprechend anzuwenden ist. Der für das Mängelgewährleistungsrecht ausschlaggebende Mangelbegriff ergibt sich daher aus den §§ 434, 435 BGB. Ein datenspezifischer Mangelbegriff besteht nicht. Der allgemeine Mangelbegriff des § 434 BGB ist durch zahlreiche Fallgruppen ausdifferenziert und dabei in objektive Kriterien (z. B. für Produkte derselben Art übliche Funktionalität, Kompatibilität und Sicherheit) und subjektive Kriterien (insbesondere die vereinbarte Beschaffenheit) gegliedert. Während nach alter Rechtslage neben der Beschaffenheitsvereinbarung bzw. der Eignung zur vertraglich vorausgesetzten Verwendung (d. h. den subjektiven Kriterien) den objektiven Kriterien nur nachrangige Bedeutung zukam, sind nun grundsätzlich beide Kriterien heranzuziehen. Allerdings gilt nach wie vor, dass objektive Anforderungen nur gelten, »soweit« nicht etwas anderes vertraglich vereinbart wurde (§ 434 Abs. 3 S. 1 BGB). Deswegen und aufgrund des noch fehlenden allgemeingültigen objektiven Standards zur Bestimmung der Datenqualität empfiehlt sich eine sehr detaillierte vertragliche Regelung. Auch sog. »negative Beschaffenheitsvereinbarungen« sind empfehlenswert; also die Festlegung, welche Qualität die Daten gerade nicht haben. So kann der Datenlieferant etwa die Eignung der Daten zum Zwecke des Trainings einer KI- oder zur Verwendung in Medizinprodukten explizit ausschließen. Im Verbraucherbereich ist dabei zu berücksichtigen, dass das Abweichen von objektiven Kriterien durch subjektive Vereinbarung sehr schwierig ist, denn nach § 476 Abs. 1 S. 2 BGB muss der Unternehmer den Verbraucher ausdrücklich davon in Kenntnis setzen, dass die Kaufsache hinter den objektiven Anforderungen zurückbleibt, und der Verbraucher muss dem ausdrücklich und gesondert zustimmen.

Bei Verbrauchsgüterkaufverträgen, die einen körperlichen Datenträger zum Gegenstand haben, der ausschließlich als Träger digitaler Inhalte dient, ist nach § 475a Abs. 1 BGB das Kaufgewährleistungsrecht nicht anwendbar.

Stattdessen gelten die Vorschriften zu Verbraucherverträgen über digitale Produkte nach §§ 327 ff. BGB. Nach § 327e Abs. 1 BGB kommt es für die Mangelfreiheit jedoch ebenfalls auf die subjektiven und objektiven Anforderungen an.

Auch wenn es keine rechtsverbindliche Definition von »Datenqualität« gibt, kann man diesbezüglich auf die Begriffsdefinition in der ISO/IEC 25024[9] zurückgreifen. Danach sind unter Datenqualität das Maß bzw. der Grad zu verstehen, in dem die Merkmale der Daten explizite oder implizite Anforderungen bei ihrer Nutzung unter festgelegten Bedingungen erfüllen. Dabei wird hier nochmals im Sinne des oben ausgeführten Mangelbegriffs wiederholt, dass es sich bei den Anforderungen um ausdrücklich vereinbarte oder implizite Anforderungen handeln kann. Bei Letzteren kann es sich sowohl um objektive, vertragsunabhängige Kriterien handeln, als auch um subjektive, aus dem konkreten Vertrag abgeleitete Kriterien. Es wird darüber hinaus aber auch klar, dass die an die Daten zu stellenden Anforderungen stets im Kontext ihrer spezifischen Nutzung zu sehen sind, die deshalb unbedingt auch vertraglich fixiert werden sollte.

Folgende Kriterien können Basis sowohl von objektiven Anforderungen als auch von subjektiven Vereinbarungen sein:

- inhaltliche Vollständigkeit, Richtigkeit und Datengenauigkeit, z. B. der Grad, in dem einzelne Daten in einem festgelegten Anwendungskontext einem korrekten Wert entsprechen – etwa die korrekte Stückzahl von Waren auf einer Palette
- Geeignetheit bzw. Gebrauchsfähigkeit der Daten zum vertraglichen Zweck, z. B. wenn die Daten zur Bestimmung von monatlichen Durchschnittsmengen genutzt werden sollen, muss der Faktor Zeit beinhaltet sein
- Bestimmung des Inhalts bzw. des Informationsgehalts der vertragsgegenständlichen Daten, z. B. wenn Informationen über Produkt A vereinbart sind, können nicht Informationen über Produkt B geliefert werden (auch wenn die Informationen über Produkt B richtig sind)
- Aktualität und ggf. Aktualisierung (sowohl des genutzten Datenbestandes als auch der zur Datenverarbeitung ggf. notwendigen Software), einschließlich Gültigkeitsfrist bzw. »Verfallsdatum« der vertragsgegenständlichen Daten, falls diese an Aktualität und Nutzwert verlieren können
- rechtliche Datenqualität, also die Freiheit von Rechten Dritter (z.B. §§ 87a ff. UrhG; GeschGehG)
- datenschutzrechtliche Zulässigkeit, z. B. Einholung und Dokumentation von erforderlichen Einwilligungen durch den Datenlieferanten
- tatsächliche / technische Datenqualität, z. B. Lieferung der richtigen Datenformate, (fehlende) Strukturierung oder Aufbereitung der Daten oder Eignung für eine bestimmte Datenübertragung, wenn die Interoperabilität von Systemen gewährleistet werden soll
- Vereinbarung der Datenquelle, z. B Daten aus besonders vertrauenswürdigen Quellen

9 System- und Software-Engineering – Qualitätskriterien und Bewertung von System- und Softwareprodukten (SQuaRE) – Messung der Datenqualität

- Effizienz, d. h. inwiefern die Daten unter angemessenem Einsatz von Ressourcen gelesen und verarbeitet werden können
- Verständlichkeit, d. h. inwiefern Daten von Nutzerkreisen korrekt interpretiert und verwendet werden können

Die Aufzählung verdeutlicht, dass Gegenstand der Betrachtung nicht unbedingt nur die Daten selbst sind, sondern z. B. deren Organisation, Strukturierung oder Darstellung auch Kriterien zur Bewertung der Qualität darstellen können.

b) Beschaffenheitsvereinbarung

Vor dem Hintergrund des oben Gesagten sollten die Parteien im Hinblick auf den Nutzungszweck klar vereinbaren, welche Beschaffenheit die Daten bzw. die Datenqualität haben sollen. Dafür bietet es sich an, die Art und die Struktur der zu liefernden Datensätze genau zu beschreiben und je nach Umfang in eine Anlage aufzunehmen. Insbesondere sollte die Leistungsbeschreibung auch klar umfassen, inwiefern die Daten für bestimmte Anwendungsbereiche gerade nicht geeignet sind.

Formulierungsbeispiel: »Die vertragsgegenständlichen Daten sind in maschinenlesbarer Form und in einem für die Weiterverarbeitung durch folgende Software _____ geeigneten Format zu übermitteln. Die Daten sind zur Nutzung als _____ beabsichtigt. Im Übrigen ergibt sich die vereinbarte Beschaffenheit der Daten aus der Anlage [XY]. Die Daten eignen sich ausdrücklich nicht für _____.«

Ein Verkäufer kann tendenziell eine weitergehende Gewähr für die Richtigkeit, Vollständigkeit und Gebrauchsfähigkeit von Daten übernehmen, je größer sein Einfluss bzw. Mitwirken im Prozess der Erzeugung der Daten bzw. Erstellung der Datensätze ist. In der Regel kann der Verkäufer jedenfalls keine Gewähr für die Richtigkeit oder eine sonstige Beschaffenheit der Erkenntnisse bieten, die der Käufer aus den überlassenen Daten individuell gewinnt. Sofern möglich, sollten Beispiele aufgenommen werden, in welchen Fällen die Parteien von einem (wesentlichen) Mangel bei einem Datensatz ausgehen.

Zu berücksichtigen ist auch, dass wegen der Fokussierung des gesetzlichen Gewährleistungsrechts auf den Zeitpunkt des Gefahrübergangs etwaige danach relevante Eigenschaften ebenfalls ausdrücklich vereinbart werden müssen, z. B. die Aktualität der Daten für einen gewissen Zeitraum.

Bei Verbrauchsgüterkaufverträgen über digitale Produkte und Waren mit digitalen Elementen ist jedoch nach der neuen Gesetzeslage die Aktualisierungspflicht nach §§ 327f und 475b Abs. 4 BGB zu beachten.

c) Spezifische Vorgaben für bestimmte Datenkategorien

Abhängig von den betroffenen Datenkategorien können spezialgesetzliche Vorgaben mit Auswirkungen auf die erforderliche Datenqualität vorliegen. So bestimmt etwa AT 4.3.4 der MaRisk bestimmte Mindestanforderungen an die Datenqualität von Risikodaten regulierter Finanzinstitute. Auch in Bezug auf den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (Smart Grids) sind ggf. Besonderheiten zu beachten. Für einen breiteren Anwendungskreis relevanter wird aber ggf. die beabsichtigte Einführung von gesetzlichen Mindestanforderungen an die Datenqualität der für die Entwicklung kritische KI-Anwendungen verwendeten Datensätze. So sollen nach dem vorgeschlagenen AI-Act der EU-Kommission[10] die Trainings-, Validierungs- und Testdatensätze für Hochrisiko-KI-Systeme nicht nur fehlerfrei und vollständig, sondern auch »relevant« und »repräsentativ« sein. Datenempfänger, die den erworbenen Datensatz zu diesen Zwecken nutzen wollen, sollten die Eignung der Daten für diese Zwecke als Beschaffenheitsvereinbarung im Vertrag ausdrücklich festhalten. Datenlieferanten, die im Zweifel nicht für diese Qualitätsmerkmale (z. B. Diskriminierungsfreiheit) der Daten haften wollen, sollten die Eignung der Daten für diese Zwecke in entsprechenden Fällen dagegen explizit ausschließen.

d) Rügeobliegenheit

Für den Handelskauf sieht § 377 HGB eine Untersuchungs- und Rügepflicht des Käufers vor, die bei Nichteinhaltung zu einem Verlust der Ansprüche für erkennbare Mängel führt. Gesetzlich sind Art und Umfang der Untersuchung nicht im Einzelnen geregelt, Vorrang haben im Rahmen des AGB-rechtlich Zulässigen jedoch vertragliche Regelungen. Die Parteien sollten daher zur Vermeidung von Rechtsunsicherheiten genau festlegen, in welcher Form und Frist die vereinbarte Beschaffenheit durch den Käufer ab Lieferung der Daten überprüft und an den Verkäufer gemeldet wird.

10 Vgl. Erwägungsgrund 43 und Art. 10 der SEC(2021) 167 final.

4.7 Vertragsbeendigung

Während für personenbezogene Daten ein Anspruch auf Löschung in Art. 18 DS-GVO und auf Datenübertragung in Art. 20 DS-GVO gesetzlich festgelegt ist, gewährt das Gesetz für nicht personenbezogene Daten keinen allgemeinen Herausgabe- oder Löschungsanspruch – sieht man von isolierten Regelungen zum Umgang mit Daten bei einer Vertragsbeendigung im Zusammenhang mit (B2C-)Verträgen über digitale Produkte ab (vgl. §§ 327o, 327p BGB). Vertragliche Regelungen bleiben aber möglich.
Eine Vertragsbeendigung kommt bei dem hier vorliegenden Fall eines Datenkaufs im Falle eines Rücktritts im Rahmen der Gewährleistung in Betracht oder sofern dies zwischen den Parteien gesondert vereinbart ist. Grundsätzlich gilt, dass bei einem Rücktritt das Recht zur Nutzung der Daten erlischt, die Daten zurückzugewähren und gezogene Nutzungen herauszugeben sind (§ 346 BGB). In der Praxis kann es hierbei zu Problemen kommen, wenn der Erwerber aus den (mangelhaften) Daten abgeleitete Daten entwickelt oder sonstige Arbeitsergebnisse unter Verwendung der Daten erzielt hat. Die bloße Herausgabe oder Löschung der Daten wird häufig nicht möglich sein oder den Interessen der Parteien nicht gerecht werden. Mögliche Regelungsgegenstände neben den Voraussetzungen der Vertragsbeendigung und der Datenrückgabe, Datenlöschung oder die Aufteilung eines gemeinsamen Datenbestandes sind daher auch, wie mit diesen Fällen umgegangen werden soll. Es gilt überdies zu berücksichtigen, dass es dem Verkäufer häufig nicht oder allenfalls schwer möglich sein wird, nachzuvollziehen, ob Daten tatsächlich gelöscht wurden oder ob Datenbestände bei einer Rückgabe nicht vorher kopiert wurden – insofern stellt sich die Situation jedoch nicht grundsätzlich anders dar als bei Verträgen über (sonstige) digitale Inhalte. Sofern für den Verkäufer erhebliche wirtschaftliche Risiken durch eine nicht rechtskonforme Behandlung der Daten entstehen können, empfiehlt sich eine vertragliche Regelung, wonach der Verkäufer – ggf. auf seine Kosten – die entsprechenden Systeme durch einen vereidigten und zur strikten Verschwiegenheit verpflichteten Sachverständigen prüfen lassen darf.

Demgegenüber ist es beim einmaligen Austausch von Datensätzen, die dauerhaft genutzt werden dürfen und für die einmalig eine Vergütung erfolgt, in der Regel nicht erforderlich oder sinnvoll, Regelungen zur Kündigung oder Laufzeit des Vertrags – mithin zur ausschließlich in die Zukunft gerichteten – Beendigung des Vertragsverhältnisses zu treffen. In Ausnahmefällen kann das Recht des Datengebers, die Nutzungsrechte nachträglich entfallen zu lassen, jedoch gewünscht sein, etwa als Sanktionsmöglichkeit zur Absicherung von Geheimhaltungsverpflichtungen oder (sonstigen) Nebenpflichten. Vor dem Hintergrund der kaufrechtlichen Einordnung des vorliegenden Vertrags und den (deutschen) AGB-rechtlichen Beschränkungen, dürfte sich von Beendigungsmöglichkeiten jedoch lediglich zurückhaltend Gebrauch machen lassen.

4.8 Geheimhaltung / Vertraulichkeit, Datensicherung und IT-Sicherheit

In entsprechenden Vertraulichkeitsvereinbarungen sollten die Daten bzw. die Informationen zu den Daten, die dem Geheimnisschutz unterliegen sollen, ausdrücklich genannt werden. Ausdrücklich ausgenommen werden müssen die Vertraulichkeitsverpflichtungen für Daten, deren Veröffentlichung aufgrund der vereinbarten Rechtseinräumung ausdrücklich erlaubt ist. Es müssen angemessene technische und organisatorische Maßnahmen zum Schutz der als Geschäftsgeheimnis vereinbarten Informationen getroffen worden sein, z. B. welche technischen Standards dafür zugrunde gelegt werden sollen und wie sicher der Datenzugang gestaltet sein muss. Die Parteien werden in der Regel schon ein hohes Eigeninteresse an derartigen Maßnahmen der Datensicherung und der IT-Sicherheit haben, um den unberechtigten Zugriff auf die Daten auszuschließen und um daraus entstehende Nachteile zu vermeiden. Dazu bieten sich entsprechende vertragliche Regelungen an, allerdings gilt hier aufgrund der nicht-ausschließlichen Wirkung des Schuldverhältnisses, dass vertragliche Regelungen auch nur zwischen den Vertragsparteien und nicht gegenüber am Vertrag nicht beteiligten Dritten wirken.

Es besteht jedoch die Möglichkeit, den Vertragspartner für die Sicherstellung und Einhaltung bestimmter Maßnahmen verantwortlich zu machen und somit zumindest faktisch eine »quasi-absolute Zuordnung« der Daten zu erreichen. Ein weiterer Vorteil von vertraglichen und tatsächlichen (physikalischen) Schutzmaßnahmen ist die Ermöglichung von Ansprüchen aus dem GeschGehG (vgl. dazu Teil 1 des Leitfadens, Ziff. 4.3. Schutz von Geschäftsgeheimnissen). Als mögliche Regelungen sind denkbar:

- Verpflichtung zur Einhaltung definierter technisch-organisatorischer Maßnahmen, z. B. Verschlüsselung der zur Verfügung gestellten Daten, Passwortschutz, eingeschränkte Zugriffsrechte an bestimmte Personen des Vertragspartners (Berechtigungskonzept), keine Speicherung der Daten in der Cloud oder in bestimmten Ländern
- Verpflichtung gegen Herausgabeverlangen Dritter (z. B. staatlicher Stellen) gerichtlich vorzugehen und den Dateninhaber über derartige Verlangen unverzüglich zu informieren
- Sofern doch eine Weitergabe an bestimmte Dritte gestattet ist, kann der Vertragspartner zur Weitergabe der vertraglich vereinbarten Maßnahmen verpflichtet werden (»Flow down«).
- Vertragsstrafen bei Verstoß gegen die vorgenannten Pflichten können geboten sein, zumal ein Schadensnachweis in der Regel schwierig zu erbringen sein wird.
- Kontrollrechte (Audit) des Dateninhabers bezüglich der Einhaltung der Sicherheitsmaßnahmen

Letztlich wird man bei der Auswahl und Ausgestaltung derartiger Regelungen differenzieren nach Art und Inhalt des vertragsgegenständlichen Datenbestandes müssen.

4.9 Datenschutz

Wie eingangs erwähnt soll der Fokus dieses Leitfadens auf nicht-personenbezogenen Daten liegen. Dieser Themenkomplex sollte jedoch auch bei rein unternehmensbezogenen Daten nicht aus dem Vertrag ausgeblendet werden. Jedenfalls sollte der Vertrag explizit klarstellen, dass die Überlassung personenbezogener Daten gerade nicht Gegenstand des Vertrags ist.

Die Frage, ob personenbezogene Daten vorliegen oder nicht, kann teilweise schwierig zu beantworten sein. Insbesondere bei der Überlassung anonymisierter Daten besteht ein Risiko, dass durch eine unzureichende Anonymisierung über Quasi-Identifikatoren oder verkettungsermöglichende Informationen eine Re-Identifizierung möglich bleibt. Ein vertragliches Verbot, die überlassenen Daten mit Daten aus anderen Datenquellen zusammenzuführen, wird in Grenzbereichen nicht ausreichen, um die Personenbeziehbarkeit (und damit die Anwendung der datenschutzrechtlichen Pflichten) zu verneinen. Lediglich überblicksartig sollen nachfolgend – ohne Anspruch auf Vollständigkeit – einige Punkte erwähnt werden, die geregelt werden müssen, wenn Datenschutzrecht auf den überlassenen Datensatz anwendbar ist:

- Die Verarbeitung personenbezogener Daten muss aufgrund einer Rechtsgrundlage nach Art. 6 DS-GVO erfolgen.
- Es sind die datenschutzrechtlichen Rollen zu bestimmen. Für die Abgrenzung von Verantwortlichen und Auftragsverarbeitern verweisen wir auf den Leitfaden ↗ »Begleitende Hinweise zu der Anlage Auftragsverarbeitung«. Die Auftragsverarbeitung muss gemäß Art. 28 Abs. 3 DS-GVO auf Grundlage eines Vertrages oder eines anderen Rechtsinstruments erfolgen (siehe z.B. die ↗ Mustervertragsanlage nach Art. 28 Abs. 3 DS-GVO).
- Den Verantwortlichen treffen gegenüber dem Betroffenen verschiedene Informationspflichten nach Art. 13, 14 DS-GVO. Zum Inhalt und der Umsetzung der Informationspflichten finden sich ausführliche Informationen im Leitfaden ↗ »Informationspflichten«. Verantwortliche und Auftragsverarbeiter müssen die Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO dokumentieren (ausführliche Informationen hierzu finden sich im Leitfaden ↗ Das Verarbeitungsverzeichnis«).
- Soweit eine vertragsgegenständliche Datenverarbeitung die Voraussetzungen einer gemeinsamen Verantwortlichkeit nach Art. 26 DS-GVO erfüllt (Joint-Controllership), müssen die Parteien in der Vereinbarung in transparenter Form festlegen, wer welche Verpflichtung gemäß der DS-GVO erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person sowie die Transparenzpflichten angeht (siehe hierzu die ↗ Checkliste für Verträge zu Joint Controllership).

Formulierungsbeispiel: »Bei den vertragsgegenständlichen Daten handelt es sind nicht um personenbezogene Daten im Sinne der EU-Datenschutzgrundverordnung.«

4.10 Haftung

Im Zusammenhang mit der dauerhaften Überlassung von Daten gegen Vergütung sind unterschiedliche Haftungsszenarien denkbar.

Haftungsauslösendes Ereignis kann insbesondere die ganz oder teilweise Nicht-Lieferung von Daten sein. Eine Haftung kann sich auch daraus ergeben, dass die Daten fehlerhaft sind (↗ zu Gewährleistungsrechten für die Datenqualität siehe auch Ziffer 4.6) oder Rechte Dritter verletzen (↗ siehe hierzu auch die Ausführungen unter Ziffer 4.11 Freistellung). Daneben ist auch die Verletzung von IT-Sicherheits- oder datenschutzrechtlichen Verpflichtungen oder Geheimhaltungsverpflichtungen denkbar. Zum Beispiel, wenn die Datenplattform, mit der die verkauften Daten bereitgestellt werden, Sicherheitslücken enthält oder wenn der Verkäufer versehentlich die Daten gegenüber dem falschen Empfänger freigibt. Als haftungsauslösendes Ereignis ist auch an einen Datenverlust zu denken. Soweit vorgenannte Ereignisse vom Verkäufer zu vertreten sind, ist er hierfür nach vertraglichen und gesetzlichen Vorschriften haftbar.

Allerdings kommen auch Haftungsansprüche gegen den Käufer in Betracht, insbesondere bei Überschreitung der vertraglich eingeräumten Datenzugangs- und Datenverwertungsrechte oder bei der Verletzung von Vertraulichkeits- oder Datenschutzpflichten.

Die Mängelhaftung aus einem Datenlieferungsvertrag richtet sich nach den vertraglichen Regelungen und ergänzend den gesetzlichen Vorschriften des Kaufvertragsrechts. Hinsichtlich der vertraglichen Haftung ist daher insbesondere auf die Ausführungen unter ↗ Z. 4.7 hinsichtlich Gewährleistung für die Datenqualität zu verweisen. Unter den entsprechenden gesetzlichen Voraussetzungen kann der Verkäufer danach zur Erstattung von Schadensersatz an den Käufer verpflichtet sein. Insbesondere besteht ein Anspruch auf Schadensersatz oder Ersatz vergeblicher Aufwendungen gemäß § 437 Nr. 3 BGB, wenn die Nachbesserung durch den Verkäufer fehlgeschlagen ist.

Der auf Seiten des Käufers denkbare Schaden (durch eine nicht oder teilweise Lieferung von Daten bzw. durch die Lieferung von Daten mit unzureichender Qualität) kann je nach Anwendungsfall stark variieren. Soweit die gelieferten Daten auf Seiten des Käufers für die Durchführung von Geschäftsprozessen oder für die Lieferung eines eigenen Produktes oder Erbringung einer Leistung erforderlich sind, sind hohe Schadenssummen denkbar. Dies dürfte anders sein, wenn Daten vorrangig für interne Zwecke (beispielsweise Marktanalyse, Marketingzwecke, Validierungszwecke) verwendet werden. Aufgrund der Vielschichtigkeit der Verwendungszwecke für Daten bietet es sich an, hinsichtlich Haftung eine ausdrückliche vertragliche Vereinbarung zu regeln, die angemessene Begrenzungen vorsieht.

Nach deutschem Recht sind dabei auch im reinen Unternehmerverkehr die Begrenzungen durch AGB rechtliche Vorschriften zu beachten. Diese führen dazu,

dass faktisch keine Haftungsbegrenzung in Allgemeinen Geschäftsbedingungen vereinbart werden kann. Um aus Sicht des Verkäufers zu einer effektiven Haftungsbegrenzung zu kommen, muss daher entweder eine individuelle Haftungsvereinbarung getroffen werden und/oder der Verkäufer führt mittelbar eine Begrenzung der Haftung durch eingrenzende Beschreibung des Vertragsgegenstands (Was wird geliefert? In welcher Qualität wird geliefert? Zu welchem Zweck dürfen die Daten verwendet werden?) herbei. Hinsichtlich des Vertragszwecks ist denkbar, auf eine sogenannte High Risk Use-Klausel zu verweisen. Solche Klauseln verbieten den Einsatz eines Dienstes für Anwendungsbereiche, in denen potenziell hohe Schäden entstehen können. Die Klausel muss allerdings so gestaltet werden, dass sie Teil der Leistungsbeschreibung wird, die keiner AGB-Kontrolle unterfällt. Die Abgrenzung zwischen Leistungsbeschreibung und Haftungsbegrenzung kann mitunter Schwierigkeiten bereiten.

Vertragliche Ansprüche des Verkäufers gegen den Käufer dürften in der Regel nach den allgemeinen Regelungen der §§ 280 ff. BGB (Schadensersatz wegen Verletzung von Pflichten aus dem Schuldverhältnis) zu bestimmen sein, wobei gegebenenfalls wirksame vertragliche Beschränkungen oder Erweiterungen (z.B. durch Garantien) zu berücksichtigen sind.

Bei gesetzlichen Ansprüchen kommen zunächst Deliktsansprüche des Käufers in Betracht. Da Daten keine Sacheigenschaft haben, dürften diese aber eher selten greifen. Eine andere Wertung könnte sich ergeben, wenn Daten von einem Datenträger gelöscht werden bzw. der Schaden durch einen sonstigen Zugriff auf Hardware des Käufers erfolgt, was jeweils als Eingriff in das Eigentum am Datenträger angesehen werden kann.

Produkthaftungsrechtliche Ansprüche dürften in der Regel auch ausscheiden, da Daten als solche kein Produkt im Sinne der Produkthaftungsrichtlinie darstellen.

Im Falle von Datenschutzverletzungen sind Schadensersatzansprüche nach Art. 82 der DS-GVO denkbar. Nach Art. 82 Abs. 1 DS-GVO hat jede Person, der wegen eines Verstoßes gegen die DS-GVO ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

Für Verletzungen von Geschäftsgeheimnissen wurde in § 10 GeschgehG ein eigenständiger Anspruch geschaffen. Die Systematik ist an das Immaterialgüterrecht angelehnt. Die Besonderheit liegt darin, dass gemäß § 10 Abs. 2 GeschgehG auch der Gewinn, den der Rechtsverletzer durch die Verletzung des Rechts erzielt hat, bei der Bemessung des Schadens berücksichtigt werden kann. Zudem kann der Schaden auch auf Grundlage einer Lizenzanalogie für die Erlangung, Nutzung und Offenlegung des Geschäftsgeheimnisses bestimmt werden. Gemäß § 10 Abs. 3 GeschgehG kann auch ein immaterieller Schaden (z. B. aus Rufschädigung oder Verlust einer Vorreiterrolle, wobei auch vertretbar ist, diese Schäden als Vermögensschäden einzuordnen) geltend gemacht werden.

4.11 Freistellung und Rechte gegen Dritte

Sofern in Bezug auf die Daten durch den Verkäufer besondere Zusagen, insbesondere zur Verhinderung von Rechtsverstößen, gegeben werden (z.B. Anonymisierung oder Aggregation, um die Daten nicht einem bestimmten Unternehmen bzw. natürlichen Personen zuzuordnen) und auch bei der Verletzung von Schutzrechten Dritter, sollten zudem Freistellungsverpflichtungen zugunsten des Käufers vorgesehen werden. Je nach Risikolage können diese auch beidseitig ausgestaltet sein (insbesondere, wenn wechselseitige Datenlieferungen erfolgen). Ausnahmsweise könnte auch vorrangig der Verkäufer ein berechtigtes Interesse an einem Freistellungsanspruch haben, z. B. zwecks Vermeidung von gesetzlichen Schadensersatzansprüchen.

Der Freistellungsanspruch sollte inhaltlich so ausgestaltet werden, dass der Käufer von allen Ansprüchen Dritter, einschließlich zuständiger Behörden sowie deren Bußgeldforderungen auf erstes Anfordern freizustellen ist und auch die angemessenen Kosten der Rechtsverteidigung zu übernehmen sind.

Schließlich kann es ratsam sein, dass sich der Verkäufer als Inhaber vertraglich geschützter, geheimer Daten gegenüber dem Käufer vorbehält, dass der Verkäufer vom Käufer informiert wird und ihm etwaige Ansprüche abgetreten werden, sofern dem Käufer wegen einer Verletzung dieser Daten Rechte gegen Dritte zustehen.

4.12 Rechtswahl, Gerichtsstand

a) Einführung

Datenkaufverträge können infolge eines Auslandsbezugs ohne entsprechende Bestimmung auch einer ausländischen Rechtsordnung unterfallen. Um mögliche Streitigkeiten wegen einer fehlenden oder unklaren Rechtswahl zu vermeiden, empfiehlt es sich, eine Rechtswahlklausel vorzusehen Mit einer Rechtswahlklausel können die Vertragsparteien die Rechtsfolgen aus ihrem Vertrag beeinflussen und unerwünschte Rechtsfolgen vermeiden. In diesem Kontext wird gerne auch die Anwendung des UN-Kaufrechts ausgeschlossen.

Schließlich empfiehlt es sich auch, einen Gerichtsstand zu bestimmen. Aus der Sicht des Datenverkäufers bietet es sich an, als Gerichtsstand den Sitz des Datenverkäufers zu wählen und dabei die ordentlichen Gerichte oder ein für passend erachtetes, schiedsgerichtliches Verfahren vorzusehen.

b) Formulierungsvorschlag

Es gilt deutsches Recht. Die Anwendung des UN-Kaufrechts ist ausgeschlossen. Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem Datennutzungsvertrag ist ____

Bitkom vertritt mehr als 2.000 Mitgliedsunternehmen aus der digitalen Wirtschaft. 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.

Bitkom e.V.

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

bitkom.org

bitkom