Herausforderung und Grenzen bei der Gestaltung von Datenverträgen

10

Sebastian Straub

Zusammenfassung

Digitale Ökosysteme leben vom Austausch und der übergreifenden Nutzung von Daten. Dem wirtschaftlichen Nutzen von digitalen Innovationen stehen häufig Sorgen vor Kontrollverlust und missbräuchlicher Verwendung von Daten gegenüber. Abhilfe schaffen technische Lösungsansätze, die den souveränen Umgang mit Daten sicherstellen und Vertrauen zwischen den Akteuren schaffen sollen. Im engen Zusammenhang hierzu steht die Frage, wem Daten rechtlich zuzuordnen sind und wer sie nutzen darf. Die bestehende Rechtsordnung gibt hierauf nur punktuell Antworten. Die Überlassung von Daten erfolgt derzeit vor allem auf Grundlage von Verträgen. Dabei gilt weitgehend das Prinzip der Vertragsfreiheit. Dies ermöglicht eine interessengerechte Ausgestaltung der Vertragsbeziehung, stellt die Vertragsparteien aber gleichzeitig vor Herausforderungen. Die lückenlose und zugleich rechtssichere Gestaltung von Datenverträgen erweist sich mitunter als schwierig. Der folgende Beitrag befasst sich mit Herausforderungen und Grenzen bei der Gestaltung von Datenverträgen.

10.1 Rechtliche Einordnung von Daten

Die juristische Einordnung von Daten stellt die Rechtsanwendenden häufig vor Herausforderungen. Die Natur von Daten lässt sich rechtlich nur schwer erfassen. Neben der syntaktischen Information in Gestalt von Zeichenfolgen, verfügen Daten regelmäßig auch über

S. Straub (✉)
Institut für Innovation und Technik (iit) in der VDI/VDE Innovation + Technik GmbH, Berlin, Deutschland
E-Mail: straub@iit-berlin.de

M. Rohde et al. (Hrsg.), *Datenwirtschaft und Datentechnologie*,
https://doi.org/10.1007/978-3-662-65232-9_10

eine semantische Ebene. Während die syntaktischen Informationen wenig Anknüpfungspunkte für eine rechtliche Beurteilung bieten, können die in Daten repräsentierten Informationen durchaus von gesetzlichen Regelungen adressiert werden. Beispielsweise unterliegen personenbezogene Informationen dem *Datenschutzrecht* oder das digitale Abbild eines literarischen Werks dem *Urheberrecht*. Unterliegen die in Daten repräsentierten Informationen einem spezifischen Regelungsregime, hat dies Auswirkungen auf die Verwertbarkeit und Handelbarkeit dieser Daten. Der bestehende Rechtsrahmen sieht jedoch, abseits der ausdifferenzierten Vorschriften im Datenschutzrecht, meist keine oder nur vereinzelte Regelungen für die wirtschaftliche Verwertbarkeit von Daten vor. Insbesondere dem *Zivilrecht* sind Eigentumsrechte oder vergleichbare absolute Rechte an Daten fremd, da diese als immaterielle Güter den sachenrechtlichen Regelungen des Bürgerlichen Gesetzbuchs (BGB) entzogen sind. Auch das *Urheberrecht* kann nur einen partiellen Schutz von Daten vermitteln. Daten als solche sind nicht schutzfähig, da ihrer Entstehung keine persönlich geistige (und damit menschliche) Schöpfung zugrunde liegt. Urheberrechtsschutz kann lediglich die Gesamtheit eines Datenbestands in Form einer Datenbank genießen. Geschützt ist in diesem Fall jedoch nur die Gesamtstruktur der Datenbank und nicht die in ihr enthaltenen Einzelinformationen. Daneben besteht ein *Leistungsschutzrecht* zugunsten des Datenbankherstellers, der eine wesentliche Investitionsleistung in die Erstellung der Datenbank getätigt hat (§§ 87a ff. UrhG). Auch unternehmensrelevante Informationen können als Geschäftsgeheimnis vor unerlaubter Erlangung, Nutzung und Offenlegung geschützt sein. Schließlich können Informationen auch einem strafrechtlichen Schutz unterliegen, etwa wenn es um die Ausspähung oder Manipulation von Daten geht (vgl. §§ 202a, 303a StGB). Die genannten Vorschriften sehen punktuell Rechte und Beschränkungen in Bezug auf die Nutzung von Daten vor. Hieraus lassen sich jedoch keine abschließenden Schlussfolgerungen ziehen, wem Daten rechtlich zuzuweisen sind (s. Abschn. 9.2.2). Die Zuordnung von Daten erfolgt daher in der Praxis häufig rein faktisch. Derjenige, der die technische Verfügungsgewalt hat, kann die Weitergabe und Nutzung durch Technikgestaltung steuern. Die Sicherstellung der Datenhoheit wird dabei vor allem durch Mittel der Datennutzungskontrolle (s. Kap. 15) gewährleistet.

10.2 Gestaltung von Datenverträgen

In datenbasierten Wertschöpfungsketten ist eine rein technische Kontrolle der Datennutzung jedoch nicht ausreichend. Das gilt für einfache bilaterale Verhältnisse zwischen Datengebenden und Datennutzenden, aber auch für komplexe Anwendungsszenarien mit einer Vielzahl von Akteuren. Notwendig sind Verträge, die die wesentlichen Rechte und Pflichten zwischen den Beteiligten regeln und die im Falle von Pflichtverletzungen konkrete Rechtsfolgen vorsehen. Daneben wird in vertraglichen Vereinbarungen die Art und Weise des Datenaustausches festgelegt. Damit wird auch im Hinblick auf die technischen Umstände der Datenüberlassung für die notwendige Rechtssicherheit gesorgt.

10.2.1 Vertragsart

Geht es um die Gestaltung von Datenverträgen, können die im BGB normierten Vertragstypen wie Kauf-, Pacht-, oder Tauschvertrag als grober Orientierungsrahmen herangezogen werden. Dabei muss jedoch berücksichtigt werden, dass diese Vertragsarten zumeist nur mittelbar auf Rechtsgeschäfte mit Daten übertragbar sind. Dennoch haben sich Begriffe wie Datenkauf oder Datenpacht teilweise etabliert (Stender-Vorwachs und Steege 2018, S. 1363). Diese Kategorisierung lässt bereits grob die Art und den Umfang der möglichen Datenüberlassung erahnen. Beim *Datenkauf* erhält die Datenempfängerin oder der Datenempfänger die dauerhafte Nutzungsmöglichkeit am Datenbestand, wodurch ein endgültiger Inhaberwechsel herbeigeführt werden soll (Schur 2021, Rn. 9). Die erwerbende Person soll im Ergebnis also eine eigentumsähnliche Position erlangen, die ihm ein vollumfängliches Verfügungsrecht sichert. Nach Maßgabe von § 453 BGB sind die Vorschriften des Kaufrechts auch auf Daten (als sonstige Gegenstände) anwendbar (Hoeren 2013, S. 489).

Demgegenüber werden Rechtsgeschäfte, die lediglich eine vorrübergehende Überlassung von Daten vorsehen, als *Datenpacht oder -miete* angesehen. Das Nutzungsrecht an den vertragsgegenständlichen Daten ist danach zeitlich beschränkt. Durch die Möglichkeit, die Nutzungsdauer und ggf. zusätzlich den Nutzungsumfang zu begrenzen, wird daher in diesem Zusammenhang in Anlehnung an das Immaterialgüterrecht auch von *Datenlizenz* gesprochen (Schur 2020, S. 1142 ff.). Bei der Überlassung von Daten kann eine Zuordnung zu einer normierten Vertragsart von Bedeutung sein, denn unter Umständen hängt hiervon ab, welche Rechtsfolgen im Falle einer Leistungsstörung (etwa bei Bereitstellung von fehlerhaften Daten) zur Anwendung kommen. Treffen die Vertragsparteien keine vertragliche Regelung, wie etwa im Falle einer mangelhaften Lieferung von Daten zu verfahren ist, greifen die gesetzlichen Bestimmungen. Zum Beispiel wären bei einem Datenkauf die Vorschriften des Kaufrechts anwendbar. Viele vertragliche Vereinbarungen lassen sich jedoch nicht oder nicht eindeutig einem bestimmten Vertragstyp zuordnen, da neben der reinen Datenüberlassung noch weitere Leistungen geschuldet werden. Häufig handelt es sich dann um typengemischte Verträge, also um Vereinbarungen, in denen unterschiedliche Vertragstypen kombiniert werden. Daneben steht es den Vertragsparteien auch frei, eine von den gesetzlichen Leitbildern vollständig losgelöste (sui generis) Vereinbarung zu treffen (Hoeren 2013, S. 489).

10.2.2 Bestimmung des Vertragsgegenstandes

Im Rahmen der Vertragsgestaltung sollte eingangs der Vertragsgegenstand definiert werden. Der Vertragsgegenstand beschreibt ganz grundlegend, auf was sich die vertraglichen Regelungen beziehen sollen. Die Festlegung des Vertragsgegenstands konkretisiert dabei nicht nur die Leistungspflicht, sondern gibt auch Anhaltspunkte darüber, welche gesetzlichen Regelungen im Falle von Mängeln und Pflichtverletzungen zur Anwendung gelangen

können (Kuß 2020, S. 393 Rn. 11). Bei Verträgen, die die Überlassung von Daten regeln, kann die Bestimmung des Vertragsgegenstands eine Herausforderung darstellen, denn Daten sind aufgrund ihrer fehlenden Verkörperung nur wenig greifbar (Froese und Straub 2021, S. 141). Umso wichtiger ist es, die zu überlassenden Datenbestände möglichst genau zu benennen. Hierzu gehört die Klärung, was unter dem Begriff „Daten" subsumiert werden soll. Um den Vertrag nicht zu überfrachten, bietet es sich an, eine ausführliche Beschreibung der vertragsgegenständlichen Daten in eine Anlage auszulagern und auf diese zu verweisen. Da Datensammlungen unter Umständen auch durch das Leistungsschutzrecht des Datenbankherstellers geschützt sein können (s. Abschn. 9.2.3), sollte eine Klarstellung erfolgen, dass auch derartige Schutzrechte vertragsgegenständlich sind. Beispielformulierung: „Gegenstand des Vertrags ist die vorrübergehende Überlassung der in Anlage 1 beschriebenen Daten, Datensammlungen und/oder Datenbanken einschließlich der jeweiligen Metadaten."

10.2.3 Einräumung von Datennutzungs- und -zugangsrechten

Als zentraler Vertragsbestandteil müssen die Parteien die Art und den Umfang der angestrebten Datennutzung bestimmen. Dabei steht die Einräumung von Datennutzungsrechten im Mittelpunkt. Enthält der Vertrag keine Bestimmungen zu Nutzungsrechten, darf die oder der Datenempfangende die Daten im Prinzip unbeschränkt für die eigenen Zwecke nutzen, da es in Bezug auf Daten gerade kein Eigentum oder ein anderes vergleichbares absolutes Recht gibt. Folglich sollte der Umfang der einzuräumenden Nutzungsrechte möglichst detailliert ausformuliert werden. Wird eine dauerhafte und unbeschränkte Überlassung der Daten angestrebt (*Datenkauf*), ist dies vertraglich festzuhalten. Durch eine derartige Vereinbarung kann die Exklusivität der Datennutzung sichergestellt werden. Ein solches Vorgehen kann dort sinnvoll sein, wo die empfangende Person sich durch die Verwertung des Datenbestands einen Wettbewerbsvorteil am Markt verschaffen möchte (von Oelffen 2020, S. 146.). Der häufiger anzutreffende Fall wird aber die zeitlich befristete Überlassung von Daten sein (*Datenpacht*), da hierdurch die Datenhoheit und die damit verbundenen Einflussmöglichkeiten des Datengebenden nicht vollständig aufgegeben werden. In diesem Zusammenhang wird auch der Begriff der *Datenlizenz* verwendet (Schefzig 2015, S. 551 ff.). Dabei ist aber zu beachten, dass durch eine Datenlizenz – im Gegensatz zu einer Lizenz im Urheberrecht – keine Rechte an einem absoluten Recht verschafft werden. Ein *absolutes Recht* ist dadurch gekennzeichnet, dass es gegenüber jedermann wirkt. Der Inhaber eines absoluten Rechts kann allein über sein Recht verfügen und Dritte von der Benutzung ausschließen. Vertraglich eingeräumte Datennutzungsrechte entfalten demgegenüber nur eine *relative Wirkung*. Der Datengeber kann etwaige Ansprüche also nur gegenüber seinem Vertragspartner (inter partes) geltend machen. Eine Rechtswirkung gegenüber Dritten entfaltet eine vertragliche Regelung nicht. Insofern hat der Datengeber in der Regel ein hohes Interesse daran, eine Datenweitergabe an Dritte zu verhindern bzw. nur dann zu gestatten, wenn hierdurch bestimmte, im Vertrag vorgese-

hene Zwecke erfüllt werden sollen. Zur Sicherstellung der Datenhoheit kann es daher empfehlenswert sein, pauschal alle nicht ausdrücklich erlaubten Nutzungshandlungen zu untersagen und die Nutzungsbefugnisse auf solche Rechte zu beschränken, die explizit vertraglich geregelt sind (Schur 2021, Rn. 22). In diesem Zusammenhang kann es auch im Interesse der Vertragsparteien liegen, den Zweck der beabsichtigten Datennutzung zu bestimmen. Zum einen hat die Festlegung des Nutzungszwecks Auswirkungen auf den Umfang der Leistungspflicht: Treffen die Vertragsparteien beispielweise eine Vereinbarung, dass die überlassenen Daten für bestimmte Zwecke nicht geeignet sind, dann hilft eine solche Festlegung bei der Auslegung im Falle von Streitigkeiten hinsichtlich des Haftungsumfangs. Zum anderen dient eine Zweckfestlegung auch dazu, gerade im Hinblick auf sensible Daten eine ausufernde Datennutzung zu unterbinden. Das kann insbesondere bei schützenswerten Unternehmensdaten wichtig sein, denn dort hat das datengebende Unternehmen in der Regel ein hohes Interesse daran, dass die überlassenen Daten nur für den im Vertrag festgelegten Zweck verwendet werden. Im Zusammenhang mit der Bestimmung von Nutzungsumfang und -zweck wird es in der Regel auch unschädlich sein, den Datenempfänger zur Löschung der Daten nach Vertragsbeendigung zu verpflichten und im Nachgang einen entsprechenden Löschnachweis einzufordern. Eine Löschungszusicherung sollte auch für den Fall vereinbart werden, wenn Verträge aufgrund von Mängeln rückabgewickelt werden müssen (Quelle: Daten im Rechtsverkehr – Überlegungen für ein allgemeines Datenvertragsrecht).

10.2.4 Datenzugang und -übertragung

Im engen Zusammenhang mit der Einräumung von Datennutzungsrechten steht die Frage des Datenzugangs. Erst wenn die technischen Umstände der Datenbereitstellung geklärt sind, können Daten genutzt und für die jeweils intendierten Zwecke verarbeitet werden. In diesem Zusammenhang sollten die Vertragsparteien die technischen Umstände der Datenüberlassung bzw. -übertragung möglichst genau festlegen. Hierzu ist es notwendig, dass Datenstandards, -formate und -schnittstellen definiert werden (Sattler 2020, S. 74 Rn. 125). Nur wenn dieses „Wie“ der Datenbereitstellung geklärt ist, lassen sich daraus verbindliche und auch rechtlich durchsetzbare Handlungspflichten ableiten. Bei der Festlegung von Übergabepunkten sind auch etwaig notwendige Mitwirkungshandlungen der Vertragsparteien zu bedenken. Ebenso sollte vertraglich festgelegt werden, wer die Kosten der Datenbereitstellung zu tragen hat (Sattler, S. 74 Rn. 125). Da die Bestimmung der technischen Umstände der Datenbereitstellung von herausragender Bedeutung ist, empfiehlt es sich, diese unter Einbeziehung der IT-Abteilung vorzunehmen (Apel 2021, Rn. 8).

10.2.5 Beschaffenheitsvereinbarung

Die Tragfähigkeit einer vertraglichen Vereinbarung zeigt sich besonders deutlich, wenn eine zugesicherte Leistung nicht oder nicht in der erwarteten Qualität erbracht wird. Im Falle einer Leistungsstörung stellt sich regelmäßig die Frage, ob und in welchem Umfang der Schuldner für die Schlechtleistung einzustehen hat. Die Beantwortung der Frage, wann Daten als vertragsgemäß anzusehen sind bzw. wann ein Mangel vorliegt, erweist sich häufig als schwierig. Der zivilrechtliche Mangelbegriff lässt sich nur teilweise auf Daten übertragen. Außerdem hängt die Brauchbarkeit von Daten sehr stark vom intendierten Verwendungszweck ab. Nicht zuletzt fehlt es häufig an Metriken zur Objektivierbarkeit der Datenqualität. Auch die Umsetzung der Digitale-Inhalte-Richtlinie (EU 2019/770) verspricht in diesem Zusammenhang keine wirkliche Klarstellung, da die dort aufgestellten Grundsätze zur Vertragsmäßigkeit digitaler Produkte (§ 327d BGB-RefE) nur im B2C-Bereich gelten. Für die Frage der Mangelhaftigkeit von Daten ist daher auf die bestehenden Regelungen des BGB zurückzugreifen. Ein *Mangel* liegt vor, wenn die Ist-Beschaffenheit von der Soll-Beschaffenheit abweicht. Für eine solche Feststellung ist es notwendig, dass die Vertragsparteien die Beschaffenheit der Daten vertraglich bestimmt haben. Festgelegt werden können beispielsweise Anforderungen zur Aktualität oder Einheitlichkeit der Daten. Die Festlegung von Mindeststandards stellt einerseits sicher, dass der oder die Datenempfangende die bereitgestellten Daten bestimmungsgemäß verarbeiten kann. Anderseits lässt sich eine Abweichung von zugesicherten Eigenschaften leichter feststellen. Die Bestimmung von konkreten Beschaffenheitskriterien ist auch deswegen von hoher Relevanz, weil sich die Mangelfreiheit von Daten ansonsten nach objektiven Kriterien bestimmt. Maßgeblich ist dann, ob die bereitgestellten Daten für den im Vertrag vorgesehenen Zweck geeignet sind. Ist keine Zweckeignung gegeben, stellt dies einen Mangel dar. Aus diesem Grund sollte neben der Bestimmung der Datenqualität auch der Verwendungszweck in den Vertrag aufgenommen werden (Schur 2021, Rn. 13; Kuß 2020, S. 414). Verzichten die Vertragsparteien hierauf, wird auf objektive Kriterien wie die übliche Beschaffenheit und Eignung zur gewöhnlichen Verwendung abgestellt. Da diese Kriterien in Bezug auf Daten schwer zu ermitteln sind, sollten die Vertragsparteien vorsorglich Beschaffenheit und Verwendungszweck vertraglich festhalten.

10.2.6 Haftung und Haftungsbeschränkung

Neben den Mängelgewährleistungsrechten ist bei der Vertragsgestaltung die Frage der Haftung- und Haftungsbeschränkung von großer Bedeutung. Grund hierfür ist, dass die überlassenen Daten häufig weiterverarbeitet werden und Grundlage für Analysen, Produkte oder Services sind. Erweisen sich Daten als fehlerhaft, kann das weitreichende Folgen haben, etwa wenn Maschinen falsch angesteuert werden und es in der Folge zu Produktionsausfällen kommt. Die Interessenslagen der Vertragsparteien sind beim Thema

Haftung in der Regel gegenläufig. Der Datenbereitsteller versucht, die Haftung weitestgehend auszuschließen oder wenigstens zu beschränken, während der Datenempfänger die Erwartung hat, für etwaige Folgeschäden eine Kompensation (meist finanzieller Art) zu erhalten. Ein Anspruch auf Schadensersatz im Rahmen eines Vertragsverhältnisses setzt zunächst voraus, dass eine Leistungspflicht verletzt wird. Besteht die (Haupt-)Leistungspflicht in der Bereitstellung von Daten in einer bestimmten Art und Güte und bleibt die tatsächliche Qualität der Daten hinter der geschuldeten Qualität zurück, kann dies im Falle eines kausalen Schadensereignisses einen Anspruch auf Schadensersatz begründen. Daraus ergibt sich die Notwendigkeit, die Beschaffenheit von Daten möglichst präzise vertraglich zu regeln (s. oben). Liegt es im Interesse einer Vertragspartei, die Haftung möglichst auszuschließen, etwa weil die Bereitstellung der Daten kostenlos erfolgt, kann auch die Festlegung einer *negativen Beschaffenheitsvereinbarung* in Erwägung gezogen werden (Kuß, S. 414, Rn. 95). Dort wird dann explizit vereinbart, dass die Qualität der Daten unterhalb eines bestimmten Niveaus liegt oder eine Eignung für bestimmte Einsatzzwecke nicht gegeben ist. Dabei gilt es aber zu beachten, dass derartige Beschaffenheitsvereinbarungen nicht im Widerspruch zum intendierten Vertragszweck stehen. Gerade bei vorformulierten Vertragsbedingungen (AGB) ist eine Freizeichnung von sogenannten „Kardinalspflichten" unzulässig. Dabei handelt es sich um Leistungspflichten, deren Verletzung den Vertragszweck gefährden würden und auf deren Erfüllung der Vertragspartner berechtigterweise vertrauen darf.

Zu beachten ist zudem, dass eine Vertragspartei nur dann schadensersatzpflichtig wird, wenn sie die Schlechtleistung zu vertreten hat. Das BGB differenziert in diesem Zusammenhang zwischen Vorsatz und Fahrlässigkeit (§ 276 Abs. 1 BGB). Im Bereich der Fahrlässigkeit wird zudem zwischen einfacher Fahrlässigkeit und grober Fahrlässigkeit differenziert. Häufig wird versucht, die Haftung für bestimmte Verschuldensformen auszuschließen. Im Grundsatz steht den Parteien dabei aufgrund der im Zivilrecht geltenden Vertragsfreiheit ein großer Handlungsspielraum zur Verfügung. Bei individuell ausgehandelten Verträgen kann die Haftung fast vollständig ausgeschlossen werden. Ausgenommen hiervon ist die Haftung für vorsätzlich herbeigeführte Schäden (§ 276 Abs. 3 BGB) oder Fälle, in denen der Ausschluss der Haftung gesetzlich untersagt ist. So ist beispielsweise der Ausschluss der Haftung für Schäden nach dem Produkthaftungsgesetz nicht möglich. Der Haftungsausschluss im Rahmen von Allgemeinen Geschäftsbedingungen (AGB) gestaltet sich demgegenüber als restriktiver. Haftungsausschlüsse bei Verletzung von Leben, Körper, Gesundheit und bei grobem Verschulden sind danach unzulässig.

10.2.7 Zusicherung von IT-Sicherheitsmaßnahmen

Eine wichtige zu erfüllende Anforderung bei der Überlassung von Daten ist die Festlegung von IT-Sicherheitsmaßnahmen. Unternehmen werden sensible Informationen nur dann bereitstellen, wenn der Datenempfänger wirksame und überprüfbare Schutzmaßnahmen zusichert, die etwa den unberechtigten Zugriff durch Dritte verhindern und die versehent-

lichen Datenfreigaben (Datenpannen) vorbeugen. Im Hinblick auf die Wahl von geeigneten IT-Sicherheitsmaßnahmen können sich die Vertragsparteien an den datenschutzrechtlichen Anforderungen der EU-Datenschutzgrundverordnung oder der ISO-Norm 27001 orientieren. Die Gewährleistung der IT-Sicherheit ist nicht nur in vertragsrechtlicher Hinsicht geboten, sondern auch vor dem Hintergrund des *Geschäftsgeheimnisschutzes* (s. Abschn. 9.2.3). Handelt es sich bei den in Daten verkörperten Informationen um Geschäftsgeheimnisse, sind diese durch das Geschäftsgeheimnisgesetz (GeschGehG) vor unberechtigter Erlangung, Nutzung und Offenlegung geschützt. Dies gilt allerdings nur, wenn der Inhaber des Geschäftsgeheimnisses angemessene Schutzmaßnahmen ergriffen hat. Hierzu gehören neben Schutzmaßnahmen technischer Natur auch die vertraglichen Maßnahmen zur Gewährleistung der Datensicherheit.

10.3 Grenzen der Vertragsgestaltung

Der Primat der Vertragsfreiheit gewährt den Akteuren in datengetriebenen Wertschöpfungsnetzen einen großen Gestaltungsspielraum. Dennoch gibt es eine Reihe von Bestimmungen, die Begrenzungen vorsehen und die bei der Vertragsgestaltung berücksichtigt werden müssen.

10.3.1 Allgemeine Geschäftsbedingungen

Werden durch die Vertragsparteien Allgemeine Geschäftsbedingungen (AGB) verwendet, so unterliegen die Bestimmungen der Inhaltskontrolle (§ 307 BGB). Bestimmungen in AGB sind unwirksam, wenn sie den Vertragspartner des Verwenders entgegen Treu und Glauben unangemessen benachteiligen. Eine unangemessene Benachteiligung kann sich daraus ergeben, dass eine Klausel nicht klar und verständlich formuliert ist und damit gegen das sogenannte Transparenzgebot verstößt. Eine unangemessene Benachteiligung ist etwa anzunehmen, wenn von wesentlichen Grundgedanken einer gesetzlichen Regelung abgewichen wird oder wesentliche Rechte und Pflichten, die sich aus der Natur des Vertrags ergeben, so eingeschränkt werden, dass die Erreichung des Vertragszwecks gefährdet ist (§ 307 Abs. 2 Nr. 1–2 BGB). Die Wahrung des Transparenzgebots kann bei Datenverträgen zu praktischen Schwierigkeiten führen. Denn diese Art von Verträgen lassen sich nur bedingt einem gesetzlich geregelten Vertragstyp zuordnen. Es fehlt in diesem Zusammenhang schlicht an einem gesetzlichen Leitbild (Kraus 2015, S. 546; Schefzig 2015, S. 563). Vor diesem Hintergrund sollten die Vertragsparteien die Leistungspflichten und den Leistungsumfang im Hinblick auf Daten besonders klar und verständlich ausarbeiten. Unklare Formulierungen und sich widersprechende Klauseln gehen zulasten des Verwenders der AGB und sollten vermieden werden.

10.3.2 Datenschutzrecht

Die Austauschbarkeit von Daten unterliegt vor allem dann Beschränkungen, wenn es sich um **personenbezogene Daten** handelt. Personenbezogene Daten sind gemäß Art. 4 Nr. 1 DSGVO „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen". Ein Personenbezug ist auch dann anzunehmen, wenn eine Identifizierung erst durch Hinzuziehung von Zusatzinformationen möglich ist (Kühling und Buchner 2020, Art. 4 Rn. 19) Bei reinen Unternehmensdaten oder Sachinformationen, die auch nicht mittelbar zu einer Identifizierung einer Person führen, ist der Anwendungsbereich der DSGVO nicht eröffnet. Die Verarbeitung von personenbezogenen Daten unterliegt strengen Vorgaben. So gebietet unter anderem der Grundsatz der *Zweckbindung*, dass Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden dürfen. Eine Sekundärnutzung zu anderen Zwecken ist nur in sehr begrenztem Umfang möglich und häufig gänzlich ausgeschlossen. Werden personenbezogene Daten datenschutzwidrig weitergegeben, kann dies Auswirkungen auf die Wirksamkeit des zugrunde liegenden Vertrags haben. Im Grundsatz sieht § 134 BGB vor, dass Rechtsgeschäfte nichtig sind, die gegen ein gesetzliches Verbot verstoßen. Erweisen sich Verträge als nichtig, können sie rückabgewickelt werden. Inwieweit Verträge bei einem Verstoß gegen das Datenschutzrecht nichtig sind, ist derzeit noch nicht höchstrichterlich entschieden. Aus Gründen der Rechtssicherheit ist bei der Vertragsgestaltung daher zu prüfen, ob personenbezogene Daten verarbeitet werden sollen. Ist das der Fall, sind die Vorgaben des Datenschutzrechts (nicht zuletzt mit Blick auf drohende Bußgelder) einzuhalten. Werden personenbezogene Daten gemeinschaftlich oder im Auftrag verarbeitet, muss der Vertrag in der Regel durch eine datenschutzrechtliche Zusatzvereinbarung (zum Beispiel einen Auftragsdatenverarbeitungsvertrag) flankiert werden.

10.4 Fazit und Ausblick

Der bestehende Rechtsrahmen gibt – vom Datenschutzrecht abgesehen – nur wenige Anknüpfungspunkte, wie Daten gehandelt oder verwertet werden können. Insbesondere fehlt es an Kriterien, welche Rechte an Daten bestehen und wem Daten zuzuordnen sind. In der Praxis erfolgt die Überlassung von Daten auf Grundlage von Verträgen. Den Vertragsparteien steht dabei ein großer Gestaltungsspielraum zur Verfügung. Grenzen bestehen dort, wo in vorhandene Schutzrechte eingegriffen oder gegen AGB- oder Datenschutzrecht verstoßen wird. Die Kehrseite der hohen Flexibilität des Vertragsrechts ist, dass die Akteure mit unterschiedlicher Verhandlungsmacht ausgestattet sind und marktschwache Akteure in Vertragsverhandlungen ins Hintertreffen gelangen könnten. Perspektivisch könnte der Einsatz von Standardvertragsklauseln die Aushandlungsposition gerade von kleinen und mittleren Unternehmen verbessern. Daneben wird voraussichtlich auch die Weiterentwicklung des Rechtsrahmens, etwa durch den EU-Data Act, die rechtlichen Rahmenbedingungen für Datenverträge beeinflussen.

Checkliste zu möglichen Vertragsbestandteilen:

- Festlegung des Vertragsgegenstands
- Einräumung von Datennutzungs- und Zugangsrechten
- Bestimmung des Nutzungszwecks
- Vereinbarung über die Löschung von Daten nach Vertragsbeendigung
- Beschaffenheitsvereinbarung
- Haftung, Haftungsbeschränkung und -ausschluss
- Zusicherung von IT-Sicherheitsmaßnahmen
- Ggf. datenschutzrechtliche Zusatzvereinbarung bei Verarbeitung von personenbezogenen Daten

Literatur

Apel S (2021) Datenkaufvertrag (3.6). In: Nägele T, Apel S (Hrsg) Beck'sche Online-Formulare IT- und Datenrecht, 7. Edition, Stand 01.05.2021. C. H. Beck, München

Froese J, Straub S (2021) Wem gehören die Daten? – Vertragliche Regelungen, Möglichkeiten und Grenzen bei der Nutzung datenbasierter Produkte. In: Hartmann EA (Hrsg) Digitalisierung souverän gestalten II – Handlungsspielräume in digitalen Wertschöpfungsnetzwerken. Springer Vieweg, Berlin, S 136–151

Hoeren T (2013) Dateneigentum – Versuch einer Anwendung von § 303a StGB im Zivilrecht. MMR: 486–491

Kraus M (2015) Datenlizenzverträge. In: Internet der Dinge – Digitalisierung von Wirtschaft und Gesellschaft, Tagungsband Herbstakademie 2015. Oldenburger Verlag für Wirtschaft, Informatik und Recht, Oldenburg, S 537–546

Kühling J, Buchner B (2020) Datenschutzgrundverordnung BDSG – Kommentar, 3. Aufl. C. H. Beck, München

Kuß C (2020) Vertragstypen und Herausforderungen für die Vertragsgestaltung. In: Sassenberg T, Faber T (Hrsg) Rechtshandbuch Industrie 4.0 und Internet of Things. C. H. Beck, München, S 387–433

von Oelffen S (2020) Gestaltung von Verträgen mit Bezug zu KI. In: Ballestrem J, Bär U, Gausling T, Hack S, von Oelffen S (Hrsg) Künstliche Intelligenz, Rechtsgrundlagen und Strategie in der Praxis. SpringerGabler, Berlin

Sattler A (2020) Schutz von maschinengenerierten Daten. In: Sassenberg T, Faber T (Hrsg) Rechtshandbuch Industrie 4.0 und Internet of Things. C. H. Beck, München, S 35–75

Schefzig J (2015) Die Datenlizenz. In: Internet der Dinge – Digitalisierung von Wirtschaft und Gesellschaft, Tagungsband Herbstakademie 2015. Oldenburger Verlag für Wirtschaft, Informatik und Recht, Oldenburg, S 551–567

Schur N (2020) Die Lizenzierung von Daten – Der Datenhandel auf Grundlage von vertraglichen Zugangs- und Nutzungsrechten als rechtspolitische Perspektive. GRUR, S 1142–1152

Schur N (2021) Datenverträge, Teil 6.9. In: Leupold A, Wiebe A, Glossner S (Hrsg) Münchener Anwaltsbuch IT-Recht, 4. Aufl. C.H. Beck, München

Stender-Vorwachs J, Steege H (2018) Wem gehören unsere Daten? – Zivilrechtliche Analyse zur Notwendigkeit eines dinglichen Eigentums an Daten, der Datenzuordnung und des Datenzugangs. NJOZ, S 1361–1367