Rechtliche Rahmenbedingungen für Big-Data- und/oder IoT-Anwendungen

Dieser Beitrag soll einen nicht abschließenden Überblick über die Schnittstellen zum Recht bei der Begleitung von Big-Data- und IoT-Anwendungen und deren Markteinführung geben. Die weitestgehende Digitalisierung hinter solchen Geschäftsmodellen stellt neue Herausforderungen an die Verteilung der Verantwortlichkeiten bei den Beteiligten. Die Frage nach Rechten an oder ein Recht auf Zugriff auf Maschinen- und personenbezogene Daten ist bei Big Data- und IoT-Anwendungen rechtlich noch nicht geklärt. Die Daten- sowie die Datenübertragungsqualität und -schnelligkeit stellen für Realtime-Anwendungen eine neue Herausforderung. Wie können diese Angebote vertragsrechtlich erfasst werden? Die engen rechtlichen Bindungen bei der Vertragsgestaltung durch das AGB-Recht im BGB können einer interessengerechten Verteilung der Verantwortlichkeiten zwischen dem Anbieter und dem Nachfrager von Big Data- und IoT-Anwendungen bei den Gewährleistungs- und Haftungsregelungen entgegenstehen. Erforderliche Standardisierungen und Interoparabilitäten sind noch offen. Dieser Beitrag gibt einen Überblick zu den rechtlichen Themen als „need to know".

1. Fallbeispiel: Ein Unternehmen aus der Branche Elektrotechnik und Maschinenbau bietet bisher Geräte und Maschinen, deren Wartung und Pflege sowie den Verkauf von Ersatz- und Verschleißteilen auch international an (nachfolgend „Hersteller"). Service-Leistungen erfolgen vielfach über einen Remote-Zugang des Herstellers zu den Geräten/Maschinen bei den Kunden vom Geschäftssitz in Deutschland aus. Neben den allgemeinen branchenspezifischen Erfahrungen sowie dem speziellen technischen und kaufmännischen Know-how des Herstellers hat dieser per Remote Zugriff auf Maschinen- und potentiell auch auf personenbezogene Daten von seinen Kunden. Der Umfang von Maschinendaten ist um das Vielfache gewachsen, nachdem der Hersteller in den letzten zwei Jahren vielfältig Sensoren und andere Datenerfassungseinrichtungen bis in die Kugellager und Beschichtungen seiner Geräte/Maschinen installiert hat. Diese Datenfülle soll nicht nur für den jeweiligen Kunden ausgewertet werden, sondern auch zu Datenbanken ausgebaut werden, in denen ebenfalls die unstrukturierten Daten durch Einsatz von Analyse-Tools in Kennzahlen und Vergleichswerte umgewandelt werden. Darauf aufbauend können dem Kunden ergänzende Leistungen wie z. B. die zeitnahe Auswertung der Produktionsdaten angeboten werden, aber auch ein anonymisiertes Bench-Marking sowie Handlungsempfehlungen und Hinweise auf vorbeugende Wartungsmaßnahmen gegeben oder später auch KI-ausgelöste Regelungen und Steuerungen angeboten werden. Eine Schnittstelle zu den Warenwirtschaftssystemen („ERP") in der IT der Kunden sowie der ERP beim Hersteller ist ein Teil der Entwicklung. Besonders die internationale Vermarktung soll über eine Cloud-Lösung für den weltweiten Zugriff auf Daten und Tools realisiert werden.

   Was sind die rechtlichen Regelungsbereiche, die sich stellen?

2. Rechtliche Rahmenbedingungen für Big-Data- und IoT-Anwendungen

2.1 Die Erfassung des Business Case

In einem ersten Schritt ist im Detail zu verstehen, welche neuen Leistungen vom Hersteller tatsächlich angeboten werden sollen. Sind dies lediglich erweiterte Dienstleistungen wie die Bereitstellung von Produktionsdaten oder der Hinweis auf einsetzende Verschleiße? Sollen automatisierte Bestellungen über Software-Agenten ausgelöst werden? Werden Informationen zu Optimierungsmöglichkeiten bei den Abläufen gegeben oder wird selbst automatisiert in Regelungen und Steuerungen beim Kunden eingegriffen? Erfolgt der Datenaustausch direkt oder soll ein Teil der Leistungen über eine Cloud-gestützte Anwendung angeboten werden? Es sind also Dienstleistungen ebenso möglicher Gegenstand einer vertraglichen Regelung mit den Kunden wie Werke im Rechtssinn oder Miete und Geschäftsbesorgung. Zudem, wo und bei wem befinden sich die Daten, die die Quelle der neuen Leistungen sein sollen? Wer hat welche Rechte hieran? Wie sind die Interessenlagen beim Hersteller und beim Kunden? Passen eingesetzte Open-Source-Software-Module (wohl immer) bei IoT-Anwendungen in das angedachte Vertriebsmodell wegen der unterschiedlichen Lizenzanforderungen verschiedener Open-Source-Lizenzwerke?

2.2 Interne Beteiligte

Es sind die Verantwortungsbereiche auf der Ebene der Unternehmensleitung berührt sowie die Tätigkeit eines möglichen Chief Data Officer, die der Entwicklung, der IT, der Bereiche Service und Vertrieb, des Controlling sowie die von Recht und, auch, Patent.

2.3 Daten = Maschinen- und personenbezogene Daten

Je nach Geschäftsmodell werden im Schwerpunkt personenbezogene oder auch personenbezogene oder nur Maschinendaten erhoben, verarbeitet und genutzt. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, § 3 Abs. 1 BDSG. Maschinendaten sind dagegen häufig unstrukturierte Daten, die beim Betrieb einer Maschine anfallen, z.B. einsatzortsabhängige Daten zu Temperatur, Licht, Feuchtigkeit, Neigung der Fläche, Erschütterungen, Umwelteinwirkungen, über Betriebsdaten des Geräts oder der Maschine bis hin zu Daten vom Zustand eines Kugellagers oder einer aufgebrachten Legierung.

Dabei sind Daten nicht gleich Informationen. Daten sind Angaben zu Sachverhalten, Informationen sind dagegen die kognitiven Schlussfolgerungen aus Daten, die also ein Wissen voraussetzen, welche semantische Aussage die Daten haben.

Maschinendaten haben keinen Bezug zu einer Person, personenbezogene Daten sind dagegen einer konkreten oder konkretisierbaren Person zuordnungsbar. Für den externen Anbieter von Datenanalyse-Anwendungen können Daten anonym sein, die aber für den Betreiber von Geräten/Maschinen bei Erhalt der Auswertungen wieder konkre-

ten Personen zugeordnet werden können, wie die Produktionsdaten zu einer bestimmten Arbeitsschicht und deren Arbeitnehmern.

An Maschinendaten kann der Eigentümer bzw. der Betreiber eines Geräts/einer Maschine ebenso Interesse haben wie der Hersteller des betreffenden Geräts oder ein Zulieferer des Eigentümers/Betreibers des Herstellers, ebenso wie für Dienstleister des Eigentümers/Betreibers.

Konflikte: Kann der Hersteller den Eigentümer/Betreiber eines Gerätes/einer Maschine technisch an einer Datensammlung hindern? Umgekehrt, kann der Betreiber den Zugriff auf Daten durch Dritte gegen den Willen des Herstellers des Gerätes/der Maschine zulassen? Darf der Hersteller anonymisierte Daten von Kunden an Dritte weitergeben?

2.4 Schutz von Daten nach geltendem Recht

Das Urhebergesetz gewährt keinen Schutz für Daten an sich. Es kennt aber einen Schutz für Datenbankwerke sowie einen Datenbankherstellerschutz, §§ 4 bzw. 87 a ff. UrhG. Letzteres ist eine Option, deren Effektivität für den Schutz der von einem Hersteller geschaffenen Datenbank(en) im Detail zu prüfen ist.

§ 17 UWG schützt Betriebs- und Geschäftsgeheimnisse. Dort ist der Schutzgegenstand aber das Geheimnis selbst. Achte: Die EU-Richtlinie 2016/943 zum vertraulichen Know-how und zu vertraulichen Geschäftsinformationen fordert in Art. 2 Nr. 1 „angemessene Schutzvorkehrungen“ als Voraussetzung für einen Geheimnisschutz. Auch hier sind nicht die Daten selbst, sondern das Geheimnis an ihnen der Schutzgegenstand.

EU-Datenfluss-Freiheit: Im VO-Entwurf der Europäischen Kommission zum freien Fluss von Rohdaten in der EU vom 13.09.2017, COM (2017) 495 final könnte Art. 6 sowie die Erläuterung zu Art. 6 und der Erwägungsgrund 11 einschlägig sein, der Anforderungen für das Angebot für Data Storage und Data Processing Services in Kombination aufstellt. Hier geht es aber um Informationspflichten, also um einen nur mittelbaren, tatsächlichen Schutz von Daten.

Das Datenschutzrecht eröffnet sich nur für der Schutz von personenbezogenen Daten im obigen Sinn.

Ein mittelbarer Schutz erfahren Daten durch das Eigentum an dem Datenträger oder einen deliktischen Schutz nach §§ 202 a, 303 a StGB, Ausspähen von Daten bzw. Datenänderungen.

Der derzeitige Stand der rechtswissenschaftlichen Diskussion verneint in der Mehrheit, dass ein Sonderrechtsschutz von Daten vom Gesetzgeber geschaffen werden sollte. Einem solchen diskutierbaren Sonderrechtsschutz steht der Grundsatz der Gemein-

freiheit von Informationen entgegen, da ansonsten eine starke Behinderung des Informationsaustauschs entstehen kann. Auch ist eine Abgrenzung zu anderen Schutzrechten schwierig. Wer sollte hier eine rechtliche Monopolstellung für welche Daten erhalten können?

Es scheint, dass dieses Thema eines möglichen selbständigen Rechtsschutzes von Rohdaten primär im deutschsprachigen Raum diskutiert wird. In den USA und in Kanada soll diese Diskussion nicht präsent sein. Es wird auf vertragliche Regelungen zu und im Zusammenhang mit Daten als Mittel eines Interessenausgleichs der Beteiligten ausgegangen.

Derzeit ist deshalb auf erforderliche vertragliche Regelungen zu Daten zwischen einem Hersteller und seinen Kunden abzustellen.

2.5 Maschinendaten des Kunden

Um Services und eine Hotline durchführen zu können, wird der Hersteller einen Remote-Zugang zu dem betreffenden Gerät/der Maschine benötigen, die z.B. vom Geschäftssitz des Herstellers erbracht werden. Dadurch erhält der Hersteller nicht nur von betriebsbezogenen Daten des Kunden Kenntnis, sondern wird diese Daten auch zur Auswertung auf einen Server herunterladen und zu seinen Servern am z.B. Geschäftssitz übertragen. Da die Berechtigung an diesen betriebsbezogenen Daten beim Kunden bisher gesetzlich nicht geregelt ist, wird wohl bisher in der Mehrzahl der Fälle der Kunde keine Einwendungen hiergegen haben, da ansonsten die Services des Herstellers nicht erbracht werden können. Mit der Gewährung des Remote-Zugriffs durch den Kunden ist deshalb die Berechtigung des Herstellers erst einmal durch Gestattung des Zugriffs geregelt. Wie verhält es sich aber, wenn der Hersteller die heruntergeladenen Daten des Kunden für eigene Zwecke nutzen und verwerten kann, indem er beispielsweise diese Daten in eine Datenbank einstellt und zum Benchmarking nutzt oder über Analyse-Tools verallgemeinerungsfähige Auswertungsmuster aufbaut? Der Kunde mag Sorge um seine Betriebs- und Geschäftsgeheimnisse haben. Auch stellt damit der Zugriff auf produktions- oder einsatzbezogene Daten des Kunden einen eigenen Wert für den Hersteller dar, sodass man an eine Vergütungspflicht denken könnte. Will der Hersteller aber den Kunden anlässlich seiner künftigen Big-Data- und IoT-Anwendungen hierauf hinweisen, um sich dann selbst zunächst viel Diskussionbedarf mit den Kunden zu schaffen? Hieran wir ein Hersteller voraussichtlich erst einmal nicht interessiert sein.

Mittelfristig wird man aber davon ausgehen können, dass der Kunde diese Thematiken für sich erkennt, sowohl bezogen auf seine Betriebs- und Geschäftsgeheimnisse als auch im Hinblick auf die Vorteile für seine eigenen Zwecke, die der Hersteller anlässlich der Services für den Kunden ziehen kann. Es ist ein Abwägen zwischen Transparenz und finanzieller Fairness einerseits sowie dem Bedürfnis, keine schlafenden Hunde zu wecken und keine vermeidbaren Diskussionen mit Kunden zu haben.

Rechtlich ließe sich für einen Interessenausgleich daran denken, dass Hersteller und Kunden anlässlich des Erwerbs des Geräts/der Maschine oder bei Abschluss von Service-Verträgen miteinander vereinbaren, dass der Hersteller berechtigt ist, Kundendaten, zu denen er per Modem Zugriff bekommt, ausschließlich anonymisiert auch für eigene Zwecke zu nutzen und der Kunde im Gegenzug hierfür eine Lizenzgebühr zum Beispiel im Wege eines Nachlasses auf den Kaufpreis oder auf die Servicegebühren erhält. Vorteil einer solchen lizenzvertraglichen Regelung kann auch sein, dass die Lizenzgewährung gegen Entgelt damit zu gegenseitigen vertraglichen Hauptleistungspflichten werden, die im Regelfall nicht einer AGB-rechtlichen Kontrolle unterliegen.

2.6 Die Geschäftsbedingungen zwischen Hersteller und Kunden bei Big-Data- und IoT-Anwendungen

2.6.1 Hersteller und Kunde sollten eine Regelung zum Umgang mit maschinen- und personenbezogenen Daten aus dem Betrieb des Geräts/der Maschine beim Kunden vereinbaren. Ist keine vertragliche Regelung vorgesehen, sondern erfolgt der Zugang und die Datenübertragung auf faktischer Ebene, spricht hierfür, dass der Kunde diese neuen Leistungsangebote des Herstellers für seinen Betrieb schlicht braucht (-en kann) und der Hersteller sonst nicht leisten kann. Der Hersteller trägt aber das Risiko, dass ihm das Recht auf Zugang und auf Nutzung und Verwertung der anlässlich des Betriebs beim Kunden anfallenden Daten auch jederzeit untersagt werden kann und damit eine Voraussetzung des Geschäftsmodells entfällt und damit der Zugang zu Maschinendaten zu seinen Geräten/Maschinen als Hersteller auf breiter Front nicht gesichert ist. Ein Weg zur Sicherung des Datenzugangs für den Hersteller und für einen Interessenausgleich mit dem Kunden wäre die zuvor vorgestellte lizenzvertragliche Regelung als eine der gegenseitigen Hauptleistungspflichten z.B. eines Kauf- oder Service-Vertrages.

2.6.2 Vertragstypologisch werden die Bereitstellung von Auswertungsergebnissen und die Aussprache von Empfehlungen, die auf Big-Data-Analysen und IoT-Anwendungen beruhen, als Dienstleistungen qualifiziert werden können. Soweit vom Hersteller Steuerungen oder Regelungen beim Betrieb des Geräts/der Maschine ausgelöst werden, werden diese Leistungen einen werkvertraglichen Charakter haben, da sie auf den Erfolg der Steuerung oder Regelung angelegt sind. Bietet der Hersteller seinem Kunden an, zum Beispiel auf einer Internet-Plattform in der Cloud selbst Analysen etc. vorzunehmen, kann es sich wie bei Software as a Service um eine mietvertragliche Regelung handeln. Ein gemischter Vertrag aus all diesen drei Leistungsarten ist ebenfalls möglich.

2.6.3 Bei der Regelung von Gewährleistung und Haftung gelten besondere Aspekte:

- Die Qualität der Daten, auf die der Hersteller Zugriff nimmt, wird wesentlichen Einfluss auf die Qualität von Analysen und Regelungen haben.

- Die Stabilität des Netzwerks, eine 100%ige Verfügbarkeit und die Schnelligkeit der Datenübertragung sind Voraussetzungen für jede Realtime-Anwendung.

- Die Nachweisbarkeit von Rechten des Herstellers an Daten kann Gegenstand einer Haftung für Rechtsmängel sein.

- Unter diesem Aspekt wirkt auch ein möglicher Know-how-Schutz für Kundendaten, die auch anonymisiert für Analysezwecke bereitgestellt werden.

- Das Recht der Allgemeinen Geschäftsbedingungen im BGB enthält eine Vielzahl von Begrenzungen der Vertragsfreiheit. Wie kann aber eine Gewährleistung für Mängel oder auch eine sonstige Haftung hierfür eingegrenzt werden, wenn das AGB-Recht dies nicht oder nur sehr begrenzt zulässt? Zum Beispiel im Hinblick auf die Qualität von Daten, die Geschwindigkeit der Übertragung und die Stabilität des Netzes sowie bei Einsatz von KI wird man Haftungsregelung lediglich durch vertragliche Zuweisung von Verantwortungen finden können. Dies wird aber zu erhöhtem Diskussionsbedarf führen.

2.6.4 Soweit auf der Ebene der Benutzeroberflächen für den Hersteller zum Beispiel das E-Mail-Account eines Arbeitnehmers beim Kunden zugänglich wird oder andere Angaben, die auch dem Hersteller es ermöglichen, eine individuelle Person zu identifizieren, ist der Zugriff auf personenbezogene Daten gegeben. Aber auch dann, wenn der Hersteller eine Anonymisierung auf der Ebene der Benutzeroberfläche technisch realisiert, kann die Auswertung zum Beispiel von betrieblichen Daten der Anlagen, etwa Störungen, Stillstände, Geschwindigkeiten etc., von dem Kunden rückverfolgt werden, sodass auch hier eine Nutzung personenbezogener Daten durch den Hersteller stattfindet und damit das Erfordernis begründet, dass die Übertragung, Bearbeitung und Nutzung dieser gegebenenfalls nur anteiligen personenbezogenen Daten den Anforderungen des Bundesdatenschutzgesetzes und künftig der Datenschutzgrundverordnung (ab 25. Mai 2018) entspricht.

2.6.5 Service Level und Reaktionszeiten auf Seiten des Herstellers bedürfen einer Regelung.

2.6.6 Dem Hersteller werden Verkehrssicherungspflichten bei Steuerungen und Regelungen eines Gerätes/einer Maschine aus seiner gesetzlichen Produkthaftung nach § 823 Abs. 1 BGB treffen.

2.6.7 Eine durchsetzbare Geheimhaltungsvereinbarung zum Schutz des Know-how und von Betriebs- und Geschäftsgeheimnissen beim Kunden ist auch unter dem Aspekt von zentraler Bedeutung, dass die EU-Richtlinie 2016/943 zum vertraulichen Know-how und zu vertraulichen Geschäftsinformationen in Art. 2 Nr. 1 „angemessene Schutzvorkehrungen“ als Voraussetzung für einen Geheimnisschutz fordert. Nachdem der Kunde dem Hersteller den Zugang zu seinen betriebsbezogenen Daten geräte- bzw. ma-

schinenspezifisch ermöglicht oder gestattet, kann eine Vertraulichkeitsverpflichtung Voraussetzung für den Fortbestand des Geheimnisschutzes sein.

2.6.8 Bei der Regelung zur Laufzeit und zur Kündigung sollte auch geregelt werden, wie der Kunde selbst Zugang zu den betriebsbezogenen Daten des Geräts/der Maschine erhält, wenn der Vertrag endet, ebenso wie welche Nutzungsrechte an Software des Herstellers enden bzw. welche Hardware möglicherweise vom Kunden herauszugeben ist, wenn sie trotz Installation beim Kunden im Eigentum des Herstellers verblieben ist.

2.7 Die Schnittstellen beim Kunden und beim Hersteller zu den jeweiligen ERP-Systemen sind zu schaffen. Ist dies eine lizenzpflichtige erweiterte Nutzung der vorhandenen ERP-Lizenz?

2.8 Eine ausreichende Ausstattung zur IT-Sicherheit beim Hersteller insbesondere an der Schnittstelle vom Hersteller zum Kunden, aber auch beim Hersteller anlässlich der Vornahme von Auswertungen/Analysen und bei Datenbanken ist eine technische Herausforderung.

2.9 Soweit der Hersteller eine Internet-Plattform für Kunden bereitstellt oder SIM-Karten in den vertriebenen Geräten/Maschinen verbaut, ist die Anwendbarkeit der Regelungen des Telemediengesetzes und des Telekommunikationsgesetzes zu prüfen, insbesondere auch im Hinblick auf die bereichsspezifischen Datenschutzregelungen.

2.10 Auf der Herstellerseite können Prozesse für Standardisierungen und die Schaffung von Interoperabilität auch unter dem Gesichtspunkt einer Gewährleistung zu verfolgen sein.

2.11 Schließlich kann zum Beispiel der Einsatz von KI-Tools dazu führen, dass auch Exportkontrollvorschriften bezogen auf bestimmte Software oder Hardware beim Vertrieb zu berücksichtigen sind.

Zusammenfassung

Besondere Herausforderung bei der vertraglichen Gestaltung von Geschäftsbeziehungen zwischen Anbietern von Big-Data- und IoT-bezogenen Anwendungen und den Anwendern in der Industrie ist die Vielgestaltigkeit der berührten Rechtsbereiche mit der Besonderheit, dass es noch keine ausgebildeten industrieüblichen Muster gibt, wie mit maschinen- und personenbezogenen Daten und den unterschiedlichen Interessen daran umzugehen ist, wie die Verantwortlichkeiten für Datenqualität, die Stabilität einer Datenübermittlung, für Fehler bei Analysen und Steuerungen/Regelungengeregelt werden können, aber dennoch die engen Grenzen des bestehenden AGB-Rechts im BGB zu berücksichtigen sind. Die fachliche Aufarbeitung beginnt erst.

München, 13.12.2017

Dr. Oliver M. Habel
Rechtsanwalt