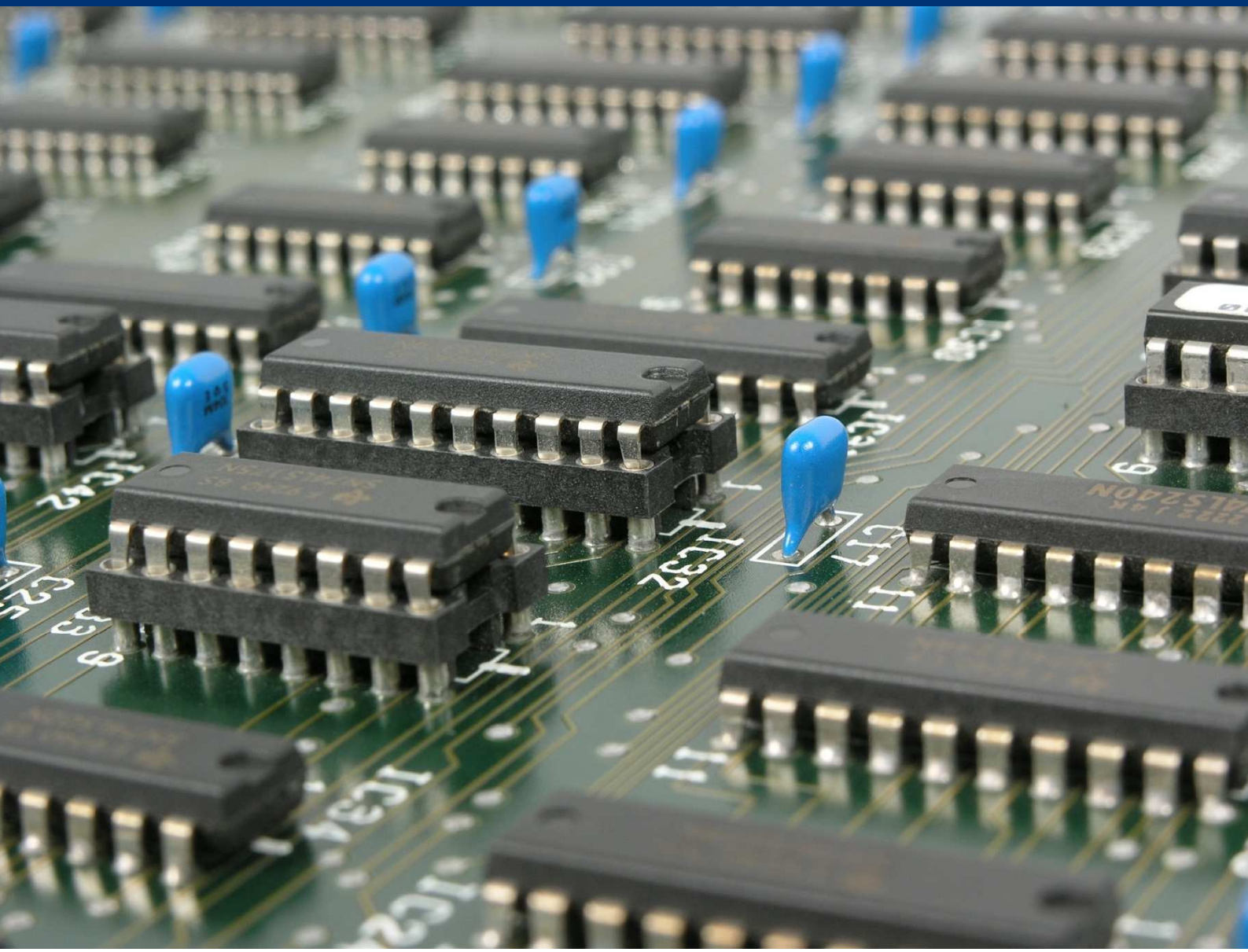
CBH
RECHTSANWÄLTE

Cornelius Bartenbach Haesemann & Partner



Industrie 4.0

Rechtliche Aspekte im Zusammenhang mit der Digitalisierung der Wirtschaft

I. Die vierte industrielle Revolution

Unter dem Begriff Industrie 4.0 wird die umfassende Vernetzung der industriellen Produktion mit moderner Informations- und Kommunikationstechnik diskutiert. Von der Digitalisierung werden alle Prozesse der Wertschöpfung erfasst – von der Produktion über die Logistik bis zur Dienstleistung. Sämtliche Prozesse sollen sich dezentral über elektronisch eindeutig identifizierbare Produkte beziehungsweise Produktkomponenten steuern lassen. Dies betrifft bestenfalls die gesamte Lebensphase eines Produktes von der Idee über die Entwicklung, Fertigung, Nutzung und Wartung bis hin zum Recycling. Im Kontext von Industrie 4.0 sollen Produktions- und Logistikprozesse künftig unternehmensübergreifend vernetzt werden, um den Informations- und Materialfluss zu optimieren. Hierdurch sollen insbesondere etwaige Fehler bzw. Störungen möglichst früh erkannt und soll auf Kundenwünsche und Marktbedingungen reagiert werden können. Modular aufgebaute Produktionsstraßen sollen innerhalb kürzester Zeit umstellbar sein, um hoch flexible und weithin automatisierte Fertigungsmöglichkeiten zu bieten. Die intelligente Fabrik der Zukunft („Smart Factory“) verfügt über moderne Informationstechnologie, standardisierte Schnittstellen („Plug & Produce“) und ist vollständig vernetzt.

Über das Internet der Dinge sind auch die Produkte selbst vernetzt und damit in der Lage, Daten mit anderen Systemen auszutauschen. Neue Trends wie „Smart Home“, „Connected Cars“ und „Smart Connected Delivery“ geben einen Hinweis darauf, wie sich die Digitalisierung zunehmend im Alltag jedes Einzelnen ausbreiten wird.

Im Ergebnis steht eine vierte industrielle Revolution bevor, nachdem bereits die Erfindung der Dampfmaschine (erste industrielle Revolution), die Einführung der Massenproduktion (zweite industrielle Revolution) und die Automatisierung durch den Einsatz von Elektronik und IT (dritte industrielle Revolution) die Industrie maßgeblich geprägt und nicht zuletzt verändert haben.

Die zunehmende Digitalisierung und Vernetzung bringen dabei enorme rechtliche Herausforderungen mit sich. Dies betrifft vor allem die Themen Datenschutz und Datensicherheit, aber auch die Bereiche Geistiges Eigentum, Haftungs- und Vertragsrecht. Zahlreiche der sich ergebenden Rechtsfragen lassen mit den bestehenden Rechtsgrundlagen lösen. In Teilbereichen, so etwa bei der Frage von Verantwortlichkeiten beim Einsatz autonomer Kraftfahrzeuge und einer etwaigen Schadensverursachung

infolge des autonomen Einsatzes, ergeben sich jedoch auch juristische Fragestellungen, die noch zu beantworten sind bzw. für die ggf. besondere gesetzliche Regelungen geschaffen werden müssen.

II. Datenschutz

Ein im Zuge von Industrie 4.0 stark betroffenes Segment ist das Datenschutzrecht. Da im Rahmen von Industrie 4.0 unterschiedlichste Bereiche vernetzt werden, bedingt dies eine zunehmende Entstehung von Daten und einen steigenden Datenfluss; dieses Phänomen wird regelmäßig unter dem Schlagwort Big Data diskutiert. Im Produktionsprozess werden in erheblichem Umfang Produktionsdaten sowie Mitarbeiterdaten generiert. Im Kontext der Nutzung von Produkten werden Produkt- und Nutzungsdaten mit zum Teil höchst sensiblem Inhalt generiert – zu denken ist hier etwa an die zunehmend verbreiteten Wearables, die oftmals gesundheitsbezogene Daten nutzen bzw. auswerten. Erhebliche Datenmengen werden auch im Zusammenhang mit Forschungs- und Wertschöpfungsprozessen – ggf. in Zusammenarbeit mehrerer Unternehmen – produziert. Die Nutzung und der Umgang mit den insoweit erzeugten bzw. erhobenen Daten werfen besondere Rechtsfragen auf.

1. Schutz personenbezogener Daten

Unternehmen, die Daten erheben, verarbeiten oder nutzen, sind grundsätzlich an die Vorgaben des Datenschutzrechts gebunden.

a) Anwendungsbereich

Dem Datenschutzrecht unterliegen allerdings nur personenbezogene Daten. Dies sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.

Im Kontext von Industrie 4.0 werden zwar vor allem technische und damit originär nicht personenbezogene Daten verarbeitet. Sobald jedoch die Möglichkeit besteht, technische Daten zu verknüpfen und diese insoweit mit einem nicht unverhältnismäßig großen Aufwand einer zumindest bestimmbaren natürlichen Person zuzuordnen, kann ein Personenbezug in Rede stehen. Da im Rahmen von Industrie 4.0 oftmals sehr große Datenmengen erzeugt bzw. gesammelt werden und immer wieder neue Datenquellen sowie Analysemöglichkeiten genutzt werden, ist es möglich, dass sich durch die Datenkumulierung neue Zusammenhänge ergeben und aus vormals lediglich technischen Daten schlussendlich doch personenbezogene Daten entstehen.

Beispiel: Connected cars

Mit dem Begriff Connected Cars werden Fahrzeuge bezeichnet, die über eine Internetverbindung verfügen und/oder zum Datenaustausch mit Smartphones oder Drittanbietern von Soft- und Hardware in der Lage sind. Werden hierbei etwa Daten über Verkehrsverhältnisse erhoben bzw. verarbeitet, liegt insoweit für sich betrachtet noch kein Personenbezug vor. Werden diese Daten jedoch mit Daten über den Aufenthaltsort des konkreten Fahrzeugs kombiniert oder lassen sich Rückschlüsse auf das Fahrverhalten des Kfz-Nutzers ziehen bzw. sogar konkret Kfz-bezogene Bewegungsprofile erstellen, sind personenbezogene Daten mit der Folge einer Anwendbarkeit datenschutzrechtlicher Bestimmung betroffen. Auch ohne eine solche Kombination liegen personenbezogene Daten dann vor, wenn der Hersteller nachvollziehen kann, welches Fahrzeug die Daten über die Verkehrsverhältnisse gemeldet hat.

b) Wie dürfen personenbezogene Daten verarbeitet werden?

Im Datenschutzrecht gilt das Verbotsprinzip mit Erlaubnisvorbehalt. Eine Verarbeitung personenbezogener Daten ist gemäß Art. 6 DS-GVO nur aufgrund einer Einwilligung der betroffenen Person oder einer gesetzlichen Legitimation zulässig.

Anonymisierung von Daten

Um das Erfordernis einer Einwilligung oder einer gesetzlichen Legitimation zu vermeiden, kommt ggf. eine Anonymisierung bzw. Pseudonymisierung betroffener Daten in Betracht. Sind Daten gemäß vollständig anonymisiert, d. h. ist ein Personenbezug nicht oder nur mit unverhältnismäßigem Aufwand herzustellen, findet die DS-GVO keine Anwendung. Die anonymisierten Daten können somit ohne Einwilligung und gesetzliche Grundlage verarbeitet bzw. genutzt werden. Im Falle einer Pseudonymisierung werden der Name oder andere Identifikationsmerkmale durch ein Kennzeichen ersetzt. Der Zweck des Ersetzens von Identifikationsmerkmalen durch neutrale Kennzeichen ist dabei darauf gerichtet, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren. Pseudonymisierte Daten sind zwar grundsätzlich auch bzw. weiterhin von der DS-GVO erfasst, jedoch kann ihre Verwendung leichter zu rechtfertigen sein.

Gesetzliche Rechtfertigungstatbestände

Erhebliche Bedeutung bei der Verarbeitung personenbezogener Daten kommt den gesetzlichen Rechtfertigungstatbeständen zu, wobei jedoch regelmäßig nur eine Nutzung in relativ engen Grenzen gestattet ist. Gerade die Digitalisierung im Rahmen von Industrie 4.0 bedingt häufig eine komplexe Nutzung personenbezogener Daten, so dass

die eigentlichen und oftmals gar nicht abschließend bestimmten Verarbeitungszwecke- bzw. Verarbeitungsmöglichkeiten durch gesetzliche Rechtfertigungstatbestände in einer Vielzahl denkbarer Konstellationen nicht gedeckt sein dürften. Jedenfalls bestünden ganz erhebliche Schwierigkeiten, insbesondere im Bereich etwaig gebotener Interessenabwägung – im Übrigen ein Problem, welches sich mit der bevorstehenden Geltung der Datenschutzgrundverordnung nicht verringern, sondern im Gegenteil verstärken wird.

Datenschutzrechtliche Einwilligung

Alternativ wird vor dem Hintergrund der Unwägbarkeiten bzw. unzureichenden Nutzungsbefugnis auf Basis gesetzlicher Erlaubnistatbestände oftmals auf Einwilligungslösungen zurückgegriffen. Eine datenschutzrechtliche Einwilligung muss vom Betroffenen auf hinreichend informierter Grundlage erklärt werden. Für den Einwilligenden ist erkennbar zu machen, welche konkreten Daten zu welchen konkreten Zwecken genutzt werden sollen. Gerade die erhebliche Komplexität und Intensität von Datenverarbeitungsvorgängen im Rahmen von Industrie 4.0 und Big Data kann zu ganz erheblichen Schwierigkeiten führen, dem Betroffenen die konkret beabsichtigte Verwendung seiner Daten verständlich und nachvollziehbar zu erläutern. Zudem ist zu bedenken, dass der Betroffene seine bereits erklärte Einwilligung jederzeit widerrufen und damit die weitere Verwendung seiner Daten unterbinden kann – oftmals ein wesentlicher Grund dafür, dass Einwilligungslösungen in der Praxis nach Möglichkeit nicht verfolgt werden.

Grundsatz der Zweckbindung

Von besonderer Relevanz im Kontext einer Datennutzung im Bereich von Industrie 4.0 ist der im Datenschutzrecht geltende Grundsatz der Zweckbindung. Jede Einwilligung bzw. Rechtfertigung erstreckt sich nach diesem Grundsatz nur auf den zunächst originär zugrundeliegenden Erhebungszweck. Sollen zu einem bestimmten Zweck erhobene Daten im Nachgang zu abweichenden Zwecken genutzt oder mit Daten aus anderen Quellen zusammengeführt werden, ist hierfür eine zusätzliche bzw. erneute Einwilligung bzw. Rechtfertigung erforderlich. Dieser Umstand erweist sich gerade im Rahmen von Industrie 4.0 und Anwendungen im Bereich Big Data als ein ganz erhebliches Hindernis, da Daten nicht selten aus ihrem ursprünglichen Zusammenhang gerissen, mit anderen Daten zusammengeführt und ausgewertet werden, wodurch letztlich neue Nutzungen bzw. Nutzungsformen begründet werden. Es bleibt abzuwarten, ob sich in der Rechtsprechung bzw. der Praxis der Aufsichtsbehörden unter der DS-GVO eine

industriefreundliche Auslegung des Zweckbindungsgrundsatzes entwickeln wird – Grund zu größerem Optimismus besteht tendenziell allerdings eher nicht.

c) Arbeitnehmerdatenschutz

Einen besonderen Problemkreis innerhalb des Datenschutzrechts stellt der Arbeitnehmerdatenschutz dar. Die zunehmende Digitalisierung in der Industrie 4.0 hat die Arbeitsabläufe für viele Arbeitnehmer bereits verändert und wird diese auch künftig verändern. In der Folge werden insbesondere auch verstärkt Arbeitnehmerdaten verarbeitet. Dabei ist zu beachten, dass das Ziel von Industrie 4.0 nicht in menschenleere Fabriken besteht. Vielmehr sollen Mensch und Maschine „zusammenarbeiten". Im Rahmen dieser Zusammenarbeit entstehen zwangsläufig und fortlaufend Daten, die nicht selten sensible Mitarbeiterdaten enthalten können, z.B. wann und wie lange sich ein Mitarbeiter an einem bestimmten Ort bzw. einer Maschine aufgehalten hat und welche Maßnahmen vom betroffenen Mitarbeiter eingeleitet bzw. gesteuert wurden („Leistungskontrolle"). Auf diese Weise lassen sich prinzipiell vollständige Bewegungs- und Nutzungsprofile über Mitarbeiter erstellen, obwohl solche Daten oftmals nur als „Abfallprodukt" im Rahmen technischer Produktions- bzw. Ablaufdokumentation anfallen.

Rechtfertigung gemäß Art. 88 DS-GVO, § 26 BDSG

Um eine Nutzung von Mitarbeiterdaten zu rechtfertigen, kommt neben der Möglichkeit der Anonymisierung dieser Daten, die softwareseitig bei entsprechender Gestaltung bereits auf der Ebene der Datenerhebung ansetzen kann („Privacy by Design" bzw. „Privacy by Default"), als gesetzliche Legitimation vor allem die insoweit datenschutzrechtlich zentrale Regelung des § 26 BDSG in Betracht. Personenbezogene Daten eines Beschäftigten dürfen nach dieser Norm für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, soweit dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach der Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Das unbestimmte Tatbestandsmerkmal der Erforderlichkeit verlangt eine Interessenabwägung und begründet in der Praxis im Einzelfall ganz erhebliche Auslegungs- bzw. Abgrenzungsschwierigkeiten.

Einwilligung im Arbeitsverhältnis oft problematisch

Ferner kann auch im Rahmen eines Arbeitsverhältnisses auf eine Einwilligungslösung zurückgegriffen werden. Insoweit werden jedoch an die für eine Einwilligung erforderliche Freiwilligkeit zuweilen hohe Anforderungen gestellt, da zwischen Arbeitgeber und

Arbeitnehmer regelmäßig ein strukturelles Ungleichgewicht besteht, was einer Freiwilligkeit im eigentlichen Sinne naturgemäß Grenzen setzt. Gleichwohl ist eine Einwilligungslösung auch im arbeitsrechtlichen Kontext keinesfalls ausgeschlossen, auch wenn das verschärfte Koppelungsverbot gemäß Art. 7 Abs. 4 DS-GVO die Rechtsmäßigkeit von Einwilligungslösungen im Arbeitsverhältnis nicht gerade erleichtern dürfte.

2. Datenschutzgrundverordnung (DS-GVO)

Die seit dem 25. Mai 2018 anzuwendende DS-GVO hat bekanntermaßen zentrale Weichen im Hinblick auf eine europaweite Vereinheitlichung des Datenschutzrechts gestellt. Dies ist angesichts oftmals länderübergreifender Datenströme im Kontext von Industrie 4.0 selbstredend begrüßenswert und auch zur Aufwandsminimierung auf Unternehmensseite zielführend. Zu beachten ist allerdings, dass die DS-GVO keine vollständige, europaweite Harmonisierung vorsieht, die einzelnen Mitgliedstaaten vielmehr über zahlreiche Öffnungsklauseln in durchaus wesentlichen Bereichen Gestaltungsspielraum nutzen können; dies betrifft etwa den besonders relevanten Bereich des Mitarbeiterdatenschutzes.

Eine insbesondere für den Bereich Industrie 4.0 und vernetzte Produkte höchst relevante Neuerung ist in der zwingenden Verpflichtung zur Berücksichtigung datenschutzrechtlicher Anforderungen und datenschutzfreundlicher Voreinstellungen bei der Konzeption von Produkten bzw. Dienstleistungen und entsprechenden Anwendungen festzumachen. Die DS-GVO sieht in Art. 25 erstmals verbindlich die bislang lediglich als Zielvorgabe geltenden Grundsätze “Privacy by Design“ (Datenschutz durch Technik) und „Privacy by Default“ (Datenschutz durch datenschutzfreundliche Voreinstellungen) vor. Im Rahmen von Privacy by Design sollen datenschutzrechtliche Anforderungen bereits bei der Produkt- bzw. Systementwicklung berücksichtigt werden, z.B. durch Beschränkung einer Datenerhebung auf anonymisierte Daten. Bei Privacy by Default sollen personenbezogene Daten auf Grundlage der bei Auslieferung eines Produkts bestehenden Grundeinstellung lediglich in einem Umfang verarbeitet werden, wie dies entsprechend dem jeweiligen Nutzungszwecke erforderlich ist; weitergehende Datennutzungen sollen dann von aktiven und für den Nutzer transparenten Einstellungsmöglichkeiten abhängen („Opt-in“). Datenschutz ist also bereits durch technische Gestaltung sicherzustellen.

III. Recht an Daten

Im Kontext von Industrie 4.0 stellt sich zudem die wirtschaftlich höchst relevante Frage, wem die anfallenden Daten gehören. Wer ist Inhaber der Daten, die von den Sensoren

einer Maschine gesammelt und von einer autonom arbeitenden Steuerung über eine Kommunikationsschnittstelle an den Server des Herstellers gesendet werden? Aufgrund der in solchen Daten verkörperten Informationen können diese einen hohen wirtschaftlichen Wert verkörpern und ein zentrales Wirtschaftsgut bilden.

Eigentum kann nach deutschem Recht nur an Sachen im Sinne von § 90 BGB bestehen, d. h. an körperlichen Gegenständen. Mangels Körperlichkeit der Daten als solcher können Eigentumsrechte grundsätzlich nur an etwaigen Datenträgern bestehen, auf denen Daten gespeichert werden. Zum Teil wird zur Begründung von Eigentum an Daten eine Anknüpfung an den technischen Herstellungsprozess der Daten mit der Folge diskutiert, dass derjenige als Eigentümer der Daten anzusehen sein soll, der die Daten generiert bzw. erstellt hat; entsprechende Ansätze werden derzeit vorwiegend im strafrechtlichen Kontext diskutiert. Nach anderer Ansicht werden entsprechende Ansätze mit der Begründung abgelehnt, dass keine Notwendigkeit für ein Eigentum an Daten bestehe, zumal die Zuerkennung eines Dateneigentums ggf. auch ungewünschte Monopolisierungswirkungen nach sich ziehen könnte.

Eine der absoluten Wirkung des Eigentumsschutzes entsprechende Zuordnung von Daten als solchen kann nach derzeit geltender Rechtslage jedenfalls nicht ohne weiteres angenommen werden. Es ist daher zu empfehlen, im Kontext von Anwendungen im Bereich Industrie 4.0 auf vertraglicher Ebene Regelungen über die Zuordnung und Verfügungsbefugnis an betroffenen Daten zu treffen. Soweit Informationen keinen absoluten Schutz besitzen, gilt es allerdings zu beachten, dass eine bloß schuldrechtliche Regelung keine Ausschließlichkeitsrechte im Hinblick auf nicht vertraglich gebundene Drittbeteiligte begründen kann. Auch die nach deutschem Recht vergleichsweise strikten Regelungen über Allgemeine Geschäftsbedingungen setzen den privatautonomen Gestaltungsmöglichkeiten Grenzen.

IV. IT-Sicherheit

Erhebliche Relevanz kommt im Rahmen der digitalisierten Wirtschaft auch dem durchaus kostentreibenden Faktor der IT-Sicherheit zu. Vor dem Hintergrund weitreichender Digitalisierung von Wertschöpfungsprozessen, der zunehmenden, oftmals auch unternehmensübergreifenden Vernetzung und dem sich entwickelnden Internet der Dinge entsteht für Hacker eine nicht zu unterschätzende Angriffsfläche. Dies gilt auch mit Blick auf die erhebliche wirtschaftliche Relevanz insbesondere größerer Datensammlungen. Beispiele aus der jüngeren Vergangenheit, die auch höchst sensible Bereiche wie etwa Datenbestände von Krankenhäusern oder etwa Zugangsdaten für Soziale

Netzwerke betrafen, belegen eindrucksvoll die Kritizität und den bestehenden Handlungsdruck. Haftet der Hersteller, wenn Hacker über eine Systemschwachstelle Zugriff auf die Kommunikationsschnittstelle eines Kfz erlangen und sicherheitsrelevante Einstellungen des Bremssystems manipulieren? Wie verhält es sich, wenn Autodiebe über eine Schadsoftware auf dem Smartphone des Halters auf eine App des Kfz-Herstellers zugreifen, mit der ein geparktes Auto geöffnet werden kann? Welche Anforderungen an die IT-Sicherheit muss der Hersteller erfüllen, um einer Haftung zu entgehen?

1. Allgemeine Vorgaben

Allgemeine bzw. verbindliche Vorgaben für die Sicherheit informationstechnischer Systeme finden sich bislang im Wesentlichen nur lückenhaft bzw. rudimentär. Pflichten zu Sicherstellung eines angemessenen IT-Sicherheitsniveaus werden primär aus allgemeinen Organisationspflichten abgeleitet, ohne dass konkrete gesetzliche Vorgaben über Art und Umfang hinreichender Sicherheitsmaßnahmen vorgegeben wären. Eine Orientierung bietet zwar der sog. Grundschutzkatalog des Bundesamtes für Sicherheit in der Informationstechnik (BSI); dieser hat jedoch im Wesentlichen Empfehlungscharakter und beansprucht keine allgemeine Verbindlichkeit. Etwas konkreter fallen die gesetzlichen Anforderungen an die IT-Sicherheit im Kontext der Verarbeitung personenbezogener Daten aus. So verpflichtet Art. 32 DS-GVO öffentliche und nicht-öffentliche Stellen im Anwendungsbereich der DS-GVO zur Umsetzung abstrakt bezeichneter technischer und organisatorischer Maßnahmen. Im Wesentlichen sind Vorkehrungen zur Sicherstellung hinreichender Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit zu treffen sowie Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung zu implementieren. Für die konkrete Umsetzung im Einzelfall bietet die DS-GVO allerdings keine konkreten Vorgaben, vielmehr haben die entsprechenden Maßnahmen in einem angemessenen Verhältnis zur Intensität einer Datenverarbeitung und der Sensibilität betroffener Daten zu stehen. Um hier aus Unternehmenssicht eine halbwegs verlässliche Grundlage schaffen und im Zweifelsfall Nachweise beibringen zu können, bieten sich entsprechende Zertifizierungen an.

2. Sicherheitsgesetz

Nicht zuletzt das Mitte 2015 in Kraft getretene Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) hat die besondere Relevanz des Themas IT-Sicherheit in den Fokus der rechtlichen Diskussion gerückt. Mit dem IT-Sicherheitsgesetz wurden insbesondere die Einhaltung von – allerdings nicht konkreten, sondern allgemein am Stand der Technik orientierten – Mindeststandards für

die IT-Sicherheit vorgeschrieben und Meldepflichten für IT-Sicherheitsvorfälle statuiert. Insoweit ist allerdings zu beachten, dass das IT-Sicherheitsgesetz nur für Betreiber sog. kritischer Infrastrukturen Geltung beansprucht. Dazu zählen namentlich die für die Gesellschaft bedeutsamen Versorgungssysteme, etwa aus den Sektoren Energie, Gesundheit, Wasser etc. Außerhalb des Anwendungsbereichs des IT-Sicherheitsgesetzes bleibt es bei den allgemeinen und wenig konkreten Vorgaben im Kontext von Organisationspflichten und Schutzmaßnahmen im Sinne des Datenschutzrechts.

3. NIS-Richtlinie

Das Thema IT-Sicherheit ist auch auf europäischer Ebene schon seit geraumer Zeit ein zentrales Anliegen. Insoweit wurde vor allem die Richtlinie zur Netzwerk- und Informationssicherheit (NIS) verabschiedet. Diese sollte im Wesentlichen zur Verbesserung der IT-Sicherheit im Bereich kritischer Infrastrukturen führen. Ziel ist ein europaweiter, einheitlicher Mindeststandard. Die Entwicklung im Bereich IT-Sicherheit ist stark im Fluss und wird auch künftig einen maßgeblichen Faktor insbesondere für Produkte und Anwendungen im Bereich Industrie 4.0 darstellen.

V. Geistiges Eigentum und Know-how-Schutz

Dem Schutz des geistigen Eigentums kommt im Zuge der Industrialisierung 4.0 ebenfalls eine zentrale Bedeutung zu. Herauszustellen ist vor allem der Schutz unternehmerischen Know-hows, welches als immaterielle Ressource nicht selten einen ganz zentralen Vermögengegenstand von Unternehmen bildet und Wettbewerbsvorteile begründet. Durch die zunehmende Digitalisierung wächst jedoch die Gefahr der unbefugten Vereinnahmung von Betriebsgeheimnissen; die steigenden Zahlen von Wirtschaftsspionage belegen dabei eindrucksvoll die Brisanz und Wichtigkeit des Know-how-Schutzes. Unternehmen sind insoweit regelmäßig darauf angewiesen, mit Geheimhaltungsvereinbarungen zu arbeiten und einen faktischen Zugangsschutz sicherzustellen.

Die bislang gesetzlich vorgesehenen Regelungen zum lauterkeitsrechtlichen Geheimnisschutz gemäß §§ 17, 18 UWG a.F. wiesen zahlreiche Lücken auf und decken selbst klassische Konstellationen von Betriebsspionage oftmals nicht hinreichend ab. Maßgebliche Änderungen im Bereich des Know-how-Schutzes brachte allerdings die „Richtlinie über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung“ mit sich, die erst unlängst und mit reichlich Verspätung in Deutschland durch das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG)

umgesetzt wurde. Das Ziel der Richtlinie besteht zentral in der Schaffung eines europaweit einheitlichen Mindeststandards zum Schutz von Betriebs- und Geschäftsgeheimnissen. Die Eröffnung des Anwendungsbereichs der Richtlinie bzw. der Schutz von Informationen unter der Richtlinie bzw. dem deutschen Umsetzungsgesetz setzt voraus, dass die betreffenden Informationen „Gegenstand von den Umständen entsprechenden angemessenen Geheimhaltungsmaßnahmen“ sind. Unternehmen, die sich auf Know-how-Schutz berufen möchten, müssen damit im Streitfall nachweisen, dass wirksame und effektive Maßnahmen zum Schutz des betreffenden Know-hows getroffen wurden. Als durchaus relevante Neuerung auf Rechtsfolgenseite ist herauszugreifen, dass der Inhaber eines Geschäftsgeheimnisses – je nach Art und Umfang einer unbefugten Verwertung dieses Geheimnisses – Rückruf- und Vernichtungsansprüche geltend machen kann.

VI. Haftung

Ein wesentlicher Ansatz von Industrie 4.0 ist auf die Umsetzung weitgehend automatisiert ablaufender Prozesse gerichtet. Soweit jedoch Prozesse auf Basis autonomer Steuerungen ablaufen bzw. Aktionen ausführen, stellt sich aus rechtlicher Sicht die Frage, wie eine angemessene Verantwortungszurechnung bzw. Verantwortungsteilung im Hinblick auf etwaige auftretende Fehler und Schäden vorzunehmen ist. Wird etwa im Rahmen einer M2M-Kommunikation (Kommunikation von Maschine zu Maschine) die relevante Kommunikationsverbindung unterbrochen und kann als Folge davon die Produktion zeitweise nicht fortgesetzt werden, stellt sich naturgemäß die Frage, wer für diesen Produktionsausfall haftet. Entsprechende Probleme sind dabei keineswegs auf den B2B-Bereich beschränkt, sondern reichen auch in den Consumer-Bereich, etwa bei Fehlfunktionen autonomer Kraftfahrzeuge bzw. autonom agierender Teilsysteme.

Solange die fehlerauslösende bzw. schadensauslösende Aktion auf eine natürliche Person bzw. auf einen bestimmten Bereich menschlichen Fehlverhaltens zurückgeführt werden kann, bietet das derzeit geltende Haftungsrecht eine hinreichende Grundlage. Neue rechtliche Herausforderungen stellen sich jedoch in Fällen, in denen vollständig autonome bzw. teilautonome Systeme Aktionen ausführen, die einer unmittelbaren Entscheidungsbefugnis und Eingriffsmöglichkeit durch den Menschen nicht zugänglich sind. Insoweit werden aktuell Modelle einer Einbeziehung entsprechender Systeme unter eine Gefährdungshaftung diskutiert. Parallel sind vertragliche Abreden und entsprechende Regelungen allerdings unabdingbar, wobei der AGB-rechtliche Rahmen im deutschen Recht gerade im haftungsrelevanten Kontext ganz erhebliche

Einschränkungen vorsieht, die einer angemessenen Regelung oftmals entgegenstehen dürften.

VII. Vertragsrechtliche Implikationen

Sofern und soweit im Kontext von Industrie 4.0 M2M-Kommunikation in dem Sinn erfolgt, dass Maschinen „Erklärungen“ abgeben, stellt sich die Frage, wie solche „Erklärungen“ zivilrechtlich einzuordnen sind, insbesondere ob insoweit vertragsrelevante bzw. rechtsverbindliche Erklärungen in Rede stehen können.

Das deutsche Recht geht von dem Prinzip aus, dass rechtsgeschäftliche Willenserklärungen von rechtsfähigen Personen abgegeben werden. Autonome Systeme sind naturgemäß nicht rechtsfähig und können daher auch keine rechtserheblichen Erklärungen abgeben. Wenn aber im Rahmen von Industrie 4.0 Maschinen autonom untereinander kommunizieren sollen, ist zu klären, ob und inwiefern diese Kommunikation rechtliche Wirkungen entfalten kann.

Beispiel: Autonome Bestellungen

Nimmt ein „selbstlernendes“ computergestütztes System eigenständig die Nachbestellung eines Ersatzteiles vor, stellt sich aus rechtlicher Sicht die Frage, ob eine entsprechende „Bestellung“ rechtlich verbindlich ist. Insoweit ist zu bedenken, dass es für den Betreiber selbstlernender autonomer Systeme nicht für jeden Einzelfall vorhersehbar sein dürfte, welchen konkreten Inhalt eine solche Kommunikation annimmt. Um hier für vertragliche Klarheit zu sorgen, ist im Kontext einer M2M-Kommunikation dringend auf vertraglicher Ebene der Erklärungswert bzw. die Verbindlichkeit von maschinellen „Erklärungen“ zu regeln. Mit adäquater Vertragsgestaltung werden sich hier Verwerfungen oftmals vermeiden oder jedenfalls deutlich entschärfen lassen.

VIII. Schlussbemerkung

Die informationstechnische Vernetzung sowie Entwicklung neuer Anwendungen im Rahmen von Industrie 4.0 stellen sowohl in tatsächlicher wie auch in rechtlicher Hinsicht neue Herausforderungen dar.

Insbesondere im Bereich des Datenschutzrechts sind im Hinblick auf die zunehmende Datenerhebung, Datenerzeugung und Datenverarbeitung vorausschauende Maßnahmen geboten, um im Nachhinein oftmals schwierig zu korrigierende Datenschutzwidrigkeiten zu vermeiden; hier kann eine stärkere Fokussierung auf Privacy by Design und Privacy by Default Abhilfe schaffen, zumal entsprechende Anforderungen nach Maßgabe der Datenschutzgrundverordnung zu beachten sein werden. Daneben ist vor

allem das Segment IT-Sicherheit zu priorisieren. Zum einen werden Maßnahmen der IT-Sicherheit als vertrauensbildender Umstand sowohl für die Zusammenarbeit von Unternehmen untereinander als auch im Verhältnis zum Endkunden als Verkaufsargument zunehmend relevant. Zum anderen können sich Unternehmen eine unzureichende IT-Sicherheit im Hinblick auf drohende Schadensszenarien sowie einen möglichen Abfluss von Geschäftsgeheimnissen bzw. sensiblen Informationen in einem digitalisierten Wirtschaftsumfeld schlicht nicht leisten.

Im Übrigen gilt es, durch vorausschauende und passgenaue Vertragsgestaltung den Herausforderungen von Industrie 4.0 insbesondere im Haftungskontext und im Zusammenhang mit Regelungen über die Zuordnung von Daten sowie zu klärende Kommunikationsflüsse zu begegnen. Ob und in welchem Umfang von Seiten des Gesetzgebers ergänzende Maßnahmen getroffen werden, ist parallel selbstredend mit besonderer Aufmerksamkeit zu beobachten.

CBH Fachbereich IT

CBH Rechtsanwälte ist eine der führenden Wirtschaftskanzleien in Deutschland und mit mehr als 90 Rechtsanwältinnen und Rechtsanwälten an den Standorten Köln, Berlin, Hamburg, München, Stuttgart und Cottbus vertreten. CBH berät in den strategischen Schwerpunktbereichen Unternehmen und Finanzen, Personal und Sozialwesen, Geistiges Eigentum, Medien und IT, Bau und Immobilien sowie Verwaltung und Wirtschaft. Mit rund 30 im Gewerblichen Rechtsschutz spezialisierten Anwälten deckt CBH das gesamte Beratungsspektrum im Bereich des Schutzes geistigen Eigentums, des Wettbewerbsrechts sowie des Medien- und IT-Rechts ab.

Unsere Tätigkeit im Fachbereich IT umfasst neben der Gestaltung komplexer Projekt- und Beschaffungsverträge in den Bereichen Hard- und Software sämtliche Beratungsleistungen für den elektronischen Geschäftsverkehr, insbesondere den Fernabsatzhandel sowie den Betrieb innovativer Portallösungen. Unsere Beratungsleistungen werden durch eine umfassende Betreuung in branchenspezifischen Angelegenheiten, etwa zu den Rahmenbedingungen des Direktmarketings, des Datenschutz- und sowie des Wettbewerbsrechts abgerundet. Wir beraten zudem bereits langjährig interdisziplinär im IT-Vergaberecht.

CBH unterstützt Sie durch individuelle und flexible Betreuung, um den im medialen und technologieorientierten Bereich stetig steigenden und sich diversifizierenden rechtlichen Anforderungen vorausschauend begegnen und auf diese Weise Betreiberrisiken minimieren zu können. Daneben berät Sie CBH bei der Planung, Durchführung und Abwicklung komplexer Projekte und ist Ihr Partner in Fällen streitiger Auseinandersetzungen. Die Möglichkeit der Einbeziehung von IT-Sachverständigen, mit welchen wir bei technischen Fragestellungen regelmäßig zusammenarbeiten, rundet unser Beratungsangebot ab.

Ansprechpartner Industrie 4.0

Dr. Sascha Vander, LL.M.
Rechtsanwalt
Fachanwalt für IT-Recht

Tel.: +49.221.951 90 - 60
Fax: +49.221.951 90 - 96
E-Mail: s.vander@cbh.de

Niklas Kinting
Rechtsanwalt

Tel.: +49.221.951 90 - 83
Fax: +49.221.951 90 - 93
E-Mail: n.kinting@cbh.de

Newsletter

Gerne informieren wir Sie mit unserem CBH-Newsletter über aktuelle Rechtsentwicklungen, Entscheidungen sowie über Veröffentlichungen und Veranstaltungen von CBH Rechtsanwälten. Wir freuen uns über Anmeldung unter www.cbh.de/newsletter

Cornelius Bartenbach Haesemann & Partner
Partnerschaft von Rechtsanwälten mbB

Köln | Berlin | Brüssel | Hamburg | München

Büro Köln
Habsburgerring 24
D-50674 Köln
Tel. +49.221.95190-0
Fax: +49.221.95190-90

E-Mail: info@cbh.de
www.cbh.de