rechtAktuell

Schwerpunkt Digitalisierung – Teil 2

LOSCHELDER

Inhalt

rechtAktuell

Schwerpunkt Digitalisierung – Teil 2

Liebe Leserinnen und Leser,

Sie halten unser zweites Sonderheft zum Thema Digitalisierung in Händen. Hiermit und mit unserer neuen Veranstaltungsreihe „Forum Digitalisierung“ begleiten Sie mit uns ein fiktives Unternehmen auf seinem Weg in die digitale Zukunft. Wir zeigen Ihnen, welche Rechtsfragen sich bei der Konzeption digitaler Produkte und Dienstleistungen stellen, wie Sie Vertragsbeziehungen im digitalen Umfeld rechtssicher gestalten und Risiken beim Aufbau Ihres digitalen Angebots minimieren. Wir besprechen mit Ihnen die Gestaltung der neuen digitalen Arbeitswelt und machen Sie fit für den digitalen Vertrieb und die Digitalisierung Ihrer Kundenbeziehungen. Schließlich veranschaulichen wir, welche neuen Herausforderungen die digitale Transformation an die unternehmensinterne Compliance stellt und wie Sie Cyberattacken und andere Krisenszenarien in digitalen Zeiten erfolgreich managen.

Termine:
Digitale Produkte & Dienstleistungen
06.11.2019, 16.00 Uhr – 18.00 Uhr

Digitale Arbeitswelt
27.11.2019, 16.00 Uhr – 18.00 Uhr

Digitaler Vertrieb
22.01.2020, 16.00 Uhr – 18.00 Uhr

Compliance & Krisenmanagement
12.02.2020, 16.00 Uhr – 18.00 Uhr

Haben wir Ihr Interesse geweckt? Ausführliche Informationen zu den Inhalten erhalten Sie unter https://loschelder.de/de/rechtsanwaelte/veranstaltungen.html oder direkt per QR-Code.

Veranstaltungsort: Loschelder Rechtsanwälte, Konrad-Adenauer-Ufer 11, 50668 Köln.

Bitte bestätigen Sie Ihre Teilnahme per Telefon oder E-Mail zwei Wochen vor der jeweiligen Veranstaltung. Ihre Ansprechpartnerin ist Frau Katrin Schwarz (katrin.schwarz@loschelder.de).

Zivilrecht

Automatisierte Vertragsschlüsse – Herausforderungen für analoges Recht in digitalen Zeiten

Die digitale Transformation ermöglicht es, unternehmensinterne Abläufe effizienter zu gestalten. Durch den Einsatz moderner Technologien lässt sich eine Vielzahl von Verfahren automatisieren, was zu signifikanten Einsparungen an Zeit und Kosten führen kann. Eine zentrale Rolle spielen dabei intelligente Maschinen, die unmittelbar miteinander kommunizieren und Daten und Informationen austauschen. Die sogenannte Machine-to-Machine-Kommunikation (M2M) hat längst Einzug in verschiedene industrielle Prozesse gefunden und ist spätestens im Zuge der Berichterstattung über die Versteigerung der 5G-Mobilfunklizenzen in das Bewusstsein einer breiten Öffentlichkeit gelangt. M2M-Kommunikation ist aber bei weitem nicht auf den unternehmensinternen Bereich beschränkt. Das Recht stellt sie vor besondere Herausforderungen insbesondere dann, wenn Maschinen nicht nur technische Daten austauschen, sondern rechtserhebliche Erklärungen abgeben und verbindliche Verträge zustande bringen sollen.

Die Grundlagen

Die Vorstellung, dass Maschinen rechtserhebliche Erklärungen abgeben, ist der Rechtsordnung im Ausgangspunkt fremd. Das Bürgerliche Recht stellt zwar grundsätzlich nur geringe Anforderungen an das Zustandekommen von Verträgen. Solange nicht im Einzelfall bestimmte Formerfordernisse bestehen, können Verträge schon durch übereinstimmendes Verhalten der Vertragspartner geschlossen werden. Es genügt, wenn aus dem Verhalten darauf geschlossen werden kann, dass die Vertragsparteien bestimmte rechtliche Wirkungen verbindlich herbeiführen wollen – sei es beim Kauf von Brötchen beim Bäcker, sei es im Zusammenhang mit der Lizenzierung hochtechnologischer Verfahrenspatente. In welcher Form oder auf welchem Übermittlungsweg die erforderlichen Willenserklärungen, Angebot und Annahme, ausgetauscht werden, ist im Grundsatz unerheblich. Eins steht jedoch seit Inkrafttreten des BGB, letztlich sogar seit der Antike unumstößlich fest: Rechtserhebliche Willenserklärungen setzen ein von einem entsprechenden Willen getragenes menschliches Verhalten voraus.

Dieses Konzept hat sich als überaus flexibel erwiesen und ist vor allem technologieneutral. Das Vertragsrecht hatte daher auch nur geringe Probleme, mit den technologischen Entwicklungen der vergangenen Jahrzehnte Schritt zu halten und konnte auch neue Vertriebsformen – wie den E-Commerce im Allgemeinen oder Internetauktionen über Ebay im Besonderen – mit den hergebrachten Instituten erklären. Aus der Sicht des Vertragsrechts bedeutete der Aufstieg des elektronischen Geschäftsverkehrs eher einen graduellen und nicht einen prinzipiellen Unterschied. Vom herkömmlichen Versandhan-

del über Telefon oder postalisch versandte Bestellformulare unterscheidet sich der Onlinehandel vor allem durch die eingesetzten Werkzeuge. In all diesen Fällen steht jedenfalls außer Zweifel, dass hinter der rechtsverbindlichen Bestellung eine menschliche Willenserklärung steht.

Die Herausforderung

M2M-Kommunikation ist anders: Ihr liegt die Idee zugrunde, dass Maschinen Daten austauschen und beim Eintreten bestimmter Voraussetzungen von sich aus bestimmte Folgeprozesse auslösen. Dabei kann es sich auch um die Abgabe einer Erklärung handeln, die zu einem rechtsverbindlichen Vertragsschluss führen soll. So ist es beispielsweise technisch möglich, dass ein Kunde über den Onlineshop eines Unternehmens eine Ware bestellt und der Eingang der Bestellung automatisch einen Herstellungsprozess auslöst, bei dem sich die vernetzten und kommunikationsfähigen Produktions-, Lager- und Logistikumgebungen untereinander austauschen und die integrierten Softwareagenten automatisiert einerseits den Transportauftrag für den Versand des fertiggestellten Produkts vergeben und andererseits die verbrauchten Rohstoffe und Vorprodukte bei den jeweiligen Lieferanten nachbestellen – und das mit jedem Bestelleingang aufs Neue und ohne, dass ein Mitarbeiter einen einzigen dieser Prozesse auslösen oder freigeben müsste.

Eine auf einen konkreten Vertragsschluss gerichtete menschliche Willenserklärung lässt sich in einem solchen Umfeld nicht mehr ohne weiteres identifizieren – erst recht nicht, wenn das eingesetzte System nicht deterministisch, sondern mit künstlicher Intelligenz arbeitet, im Laufe der Zeit hinzulernt und autonom agiert. Die digitale Transformation stellt das aus analogen Zeiten stammende Vertragsrecht daher vor Herausforderungen, an die Ende des 19. Jahrhunderts, als das BGB entstand, nicht einmal gedacht werden konnte.

Führt der Umstand, dass das BGB keine ausdrücklich auf die M2M-Kommunikation anwendbaren Regelungen kennt, aber dazu, dass rechtsverbindliche Verträge mittels Maschinenerklärungen nicht wirksam geschlossen werden können? Im Ausgangspunkt gilt, dass Willenserklärungen, die ein IT-System automatisiert abgibt, dessen Betreiber als eigene Erklärung zugerechnet werden können. Dies hat der Bundesgerichtshof für Erklärungen, die von einem EDV-gesteuerten Warenwirtschaftssystem ausgelöst werden, bereits 2005 entschieden. Und zwar zu Recht: Das Warenwirtschaftssystem sollte schließlich nur den Willen des Betreibers ausführen, den dieser zuvor gebildet und durch Pflege des zugrundeliegenden Datenbestands in der automatisierten Erklärung angelegt hatte. Für die Zurechnung automatisiert abgegebener Willenserklärungen kann es daher genügen, dass der Betreiber das IT-System willentlich in Betrieb nimmt – jedenfalls bei deterministischen Systemen, die lediglich die vordefinierten Anordnungen des Betreibers umsetzen.

An seine Grenzen stößt dieser Ansatz freilich in Bezug auf autonom agierende Systeme, bei denen der Betreiber nicht im Vorfeld abschließend festlegt, welche Erklärungen das System unter welchen Bedingungen abgibt. So ist es denkbar, dass der Bertreiber ein intelligentes IT-System für den Einkauf von Waren einsetzt, hierfür nur einen mehr oder weniger allgemeinen Rahmen vorgibt, das System hingegen über den Zeitpunkt der Abgabe und den Inhalt der Erklärung, zum Beispiel bezüglich der zu bestellenden Menge und den Angebotspreis, unter Einsatz von Big-Data-Analysen und künstlicher Intelligenz selbstständig entscheidet. Mit wachsender Autonomie

wird das Verhalten solcher intelligenter Systeme immer weniger prognostizierbar. Unter diesen Umständen ist es nicht mehr selbstverständlich, die automatisiert abgegebene Erklärung dem Bertreiber der Anlage zuzurechnen – den konkreten, maschinell geäußerten Willen hätte der Betreiber in dieser Form womöglich nie gebildet.

Die Lösung?

In der rechtswissenschaftlichen Literatur werden hierzu verschiedene Lösungsansätze diskutiert, die im Falle der Umsetzung erhebliche Eingriffe in das bisherige System des Vertragsrechts erforderlich machen würden. So wird etwa die Frage aufgeworfen, ob mit Blick auf die wachsende Autonomie von Robotern und Softwareagenten, deren Reaktionen wesentlich durch intelligentes Lern- und Kommunikationsverhalten bestimmt werden, die eigene Rechtspersönlichkeit dieser Systeme anerkannt werden sollte. In diesem Fall müsste eine neue Kategorie der „E-Person“ geschaffen werden, die neben die der natürlichen Person und der juristischen Person tritt. In eine ähnliche Richtung weisen Vorschläge, die Regeln des Stellvertretungsrechts auf Maschinenerklärungen entsprechend anzuwenden.

Ob hiermit wirklich etwas gewonnen wäre, ist allerdings zweifelhaft. Wichtige Haftungsfragen ließen sich hierdurch allein auch nicht klären. Wesentlich wahrscheinlicher ist es daher, dass der Gesetzgeber auf solch tiefgreifende Einschnitte in die Rechtsordnung verzichtet und es stattdessen der Rechtsprechung überlässt, den eingeschlagenen Weg, Maschinenerklärungen auf Grundlage der hergebrachten gesetzlichen Regelungen dem Betreiber zuzurechnen, fortzubilden. Hierfür sprechen auch Gründe der Rechtssicherheit – insbesondere für den potentiellen Vertragspartner, der häufig nicht erkennen wird, ob eine elektronisch übermittelte Erklärung von einem Menschen oder einer Maschine abgesetzt wurde.

Die Konsequenzen

Auch wenn der gegenwärtig wahrscheinlichste Lösungsansatz, das hergebrachte System des Vertragsrechts auf Grundlage bestehender Regelungen fortzuentwickeln, auf den ersten Blick vergleichsweise leicht umzusetzen erscheinen mag, ist er für den Betreiber eines autonomen IT-Systems nicht ungefährlich. Die Zurechnung autonom abgegebener Maschinenerklärungen kann zu erheblichen Haftungserweiterungen führen. Wenn dem Betreiber alle Maschinenerklärungen, die aus seiner Sphäre stammen, zugerechnet werden, ohne dass es auf dessen konkrete Willensbildung ankommt, muss er grundsätzlich für die gesamte Erklärungstätigkeit des Systems einstehen und für die sich daraus ergebenden Folgen aufkommen. Dabei kann er sich nicht darauf berufen, dass das konkrete Verhalten der Maschine für ihn nicht vorhersehbar gewesen sei. Wenn der Betreiber die Vorteile eines autonomen IT-Systems in Anspruch nehmen möchte und die Willensbildung in die virtuellen Hände einer Maschine legt, kann er sich nicht damit entlasten, dass die Inhalte der Maschinenerklärung im Einzelfall nicht seinem Willen entsprechen.

Abzuwarten bleibt, wie mit möglichen Härten umzugehen ist, die sich aus einer umfassenden Zurechnung von Maschinenerklärungen und den damit einhergehenden Haftungsfolgen ergeben könnten. Ein Weg wäre, die Möglichkeiten, fehlerhafte Erklärungen anzufechten, auszuweiten. Die bisherigen Anfechtungsgründe erfassen die Fälle maschineller „Kompetenzüberschreitungen“ nicht und greifen allenfalls bei Systemfehlern, die sich in einer fehlerhaften Übermittlung der Vorgaben des Bertreibers niederschlagen.

Mit Blick auf die Interessen des Erklärungsempfängers dürfte eine Ausweitung der Anfechtungsgründe allerdings nur unter engen Voraussetzungen sachgerecht sein.

Praxishinweis

Technisch mag die automatisierte Kommunikation zwischen Maschinen längst möglich sein und Einzug in industrielle Fertigungs-, Überwachungs- und Logistikprozesse gefunden haben. Sobald mittels M2M-Kommunikation rechtsverbindliche Erklärungen abgegeben werden, betreten alle Beteiligten hingegen weitgehend unbekanntes Gelände. Die Rechtsordnung muss befriedigende Antworten auf die Fragen, die der Einsatz autonomer IT-Systeme zum automatisierten Abschluss rechtsverbindlicher Verträge aufwirft, erst noch finden. Das gleiche gilt im Übrigen für produkthaftungsrechtliche und regulatorische Fragen der M2M-Kommunikation.

Unternehmen, die M2M-Lösungen in ihre betrieblichen Abläufe integrieren möchten, sollten daher zuvor eine gründliche Risikoanalyse durchführen, die auch Fragen der Versicherbarkeit der Risiken beinhaltet. Aber auch für potentielle Vertragspartner dieser Unternehmen führt die bis auf weiteres bestehende Rechtsunsicherheit auch dann zu erhöhtem Beratungsbedarf, wenn sie selbst keine autonomen IT-Systeme betreiben. Weitreichende unternehmerische Entscheidungen und Dispositionen kann auf einer fundierten Grundlage schließlich nur treffen, wer die rechtlichen Risiken und die sich daraus ergebenden Konsequenzen kennt.

Für sämtliche Fragen zu automatisierten Vertragsschlüssen stehen Ihnen gerne zur Verfügung:

Dr. Stefan Maaßen, LL.M.
0221 650 65-231
stefan.maassen@loschelder.de

Dr. Patrick Pommerening
0221 650 65-134
patrick.pommerening@loschelder.de

Markenrecht

Moderne Markenformen – Paradigmenwechsel mit Folgen

Wer den Begriff „Marke“ hört, denkt in erster Linie an Namen („Siemens“), Fantasiewörter („Google“) oder Logos („Nike-Swoosh“), ggf. auch an Zahlen- und Buchstabenkombinationen („RTL“). Das Markenrecht ist jedoch nicht auf den Schutz solcher typischer Zeichen, also Wortmarken oder Bildmarken, beschränkt. Als Marke können grundsätzlich alle Zeichen geschützt werden, die geeignet sind, Waren oder Dienstleistungen eines Unternehmens von denjenigen anderer Unternehmen zu unterscheiden. Dies umfasst nicht-konventionelle Markenformen, bei denen die Marke aus bestimmten Klängen, dreidimensionalen Gestaltungen, sonstigen Aufmachungen oder Farben und Farbzusammenstellungen besteht. Die praktische Bedeutung dieser sogenannten „modernen Markenformen“ ist in der Vergangenheit jedoch vergleichsweise gering geblieben. Dies könnte sich nach der jüngsten Reform des Markenrechts ändern – und Unternehmen insbesondere beim digitalen Vertrieb ihrer Produkte neue Möglichkeiten der Marktkommunikation bieten.

„Klare und eindeutige Bestimmbarkeit“ statt „grafischer Darstellbarkeit“

Der Schutz moderner Markenformen scheiterte bislang in vielen Fällen an den praktischen Vorgaben des Anmelde- und Eintragungsverfahrens. Die für die Markenanmeldung zuständigen Behörden, also das Deutsche Patent- und Markenamt (DPMA) und das Amt der Europäischen Union für geistiges Eigentum (EUIPO), ermöglichten die Eintragung eines Zeichens in das Markenregister nur unter der Voraussetzung, dass das Zeichen „grafisch darstellbar“ ist. Mit dieser Vorgabe sollte sichergestellt werden, dass der Bestand und Umfang von Marken für alle Akteure zweifelsfrei definiert und erkennbar ist.

So nachvollziehbar Sinn und Zweck dieser Regelung sind, führte das Erfordernis der grafischen Darstellbarkeit zu Beschränkungen des Schutzes moderner Markenformen, die vor dem Hintergrund der technischen Entwicklung nicht mehr gerechtfertigt waren. Zwar war es auch vor der Markenrechtsreform möglich, 3D-Marken durch verschiedene Ansichten des Gegenstands, für den Schutz beansprucht wird, registergerecht in zweidimensionaler Form darzustellen. Dennoch konnte es für Markenanmelder überaus schwierig sein, durch grafische Darstellungen den Schutzgegenstand ihrer modernen Marke präzise zu beschreiben. Einen Grund für die nicht mehr zeitgemäßen Beschränkungen gab es letztlich nicht: Das Markenregister wird bereits seit zwei Jahrzehnten elektronisch geführt, sodass auch zahlreiche andere Darstellungsformen als die grafische zur Verfügung stehen, um den Schutzgegenstand zu definieren.

Mit der jüngsten Reform des Markenrechts, die für nationale deutsche Marken am 14. Januar 2019 in Kraft getreten ist, hat der Gesetzgeber die Voraussetzungen dafür geschaffen, dass die digitale Transformation in weit größerem Maße in die Markenverwaltung Einzug erhält, als dies bislang der Fall war. Seitdem hängt die Eintragung einer Marke nicht mehr davon ab, dass sich das Zeichen grafisch darstellen lässt. Von der Eintragung als Marke sind jetzt nur noch solche Zeichen ausgeschlossen, „die nicht geeignet sind, in dem Register so dargestellt zu werden, dass die zuständigen Behörden und das Publikum den Gegenstand des Schutzes klar und eindeutig bestimmen können". Damit öffnet sich das Markensystem den technischen Möglichkeiten und lässt grundsätzlich jedes Darstellungsmittel zu, das geeignet ist, den Schutzgegenstand klar und eindeutig wiederzugeben. Dies ermöglicht den Markenschutz für Zeichen und bestimmte Merkmale von Zeichen, die zuvor aufgrund der registerrechtlichen Einschränkungen praktisch vom Markenschutz ausgeschlossen waren. Die Ämter erhoffen sich hierdurch nicht weniger als eine neue Ära beim Schutz moderner Markenformen.

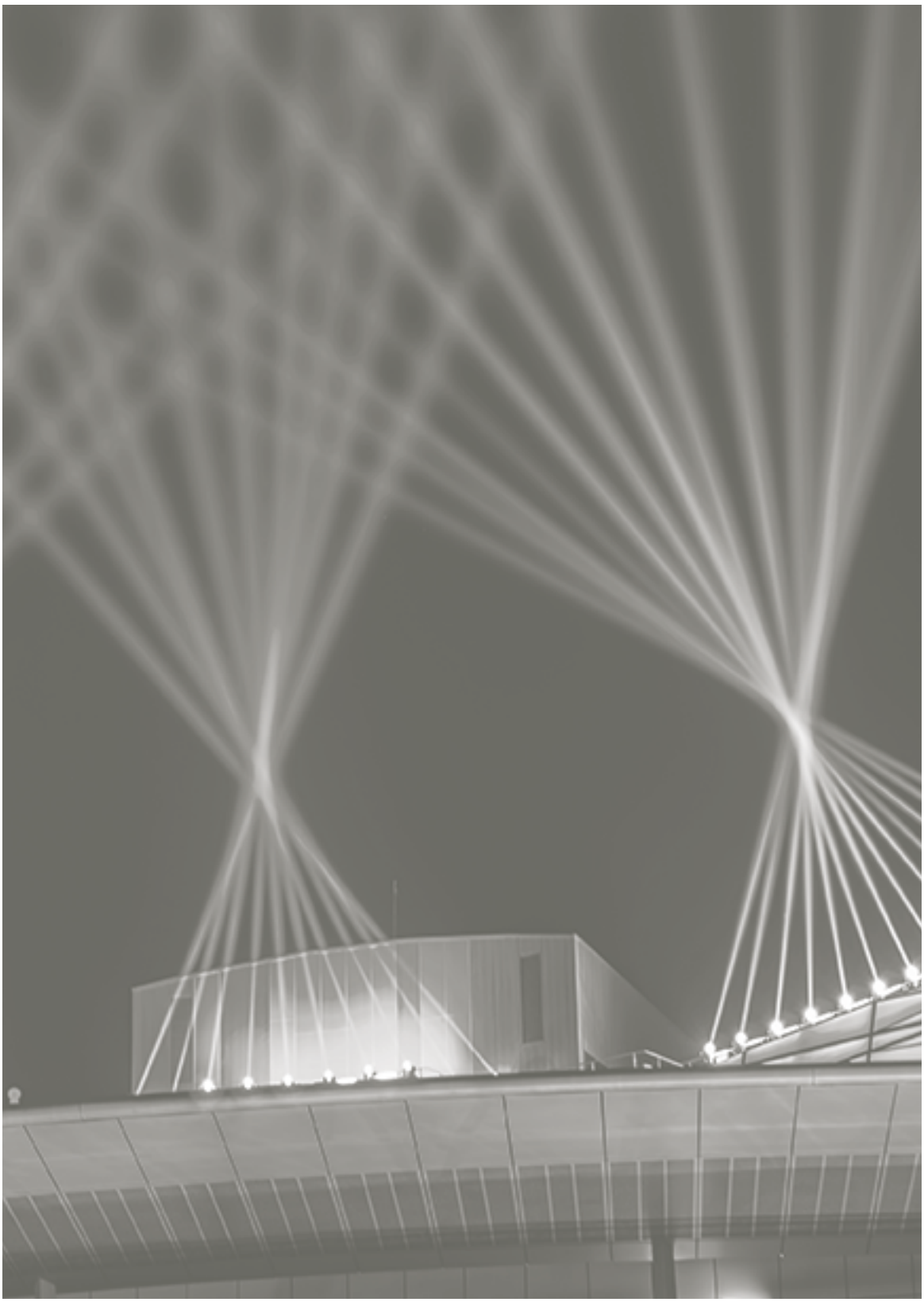
Vorgaben für einzelne Markenformen

Auch wenn das Markengesetz und die Unionsmarkenverordnung lediglich das Darstellungsziel („klar und eindeutig bestimmbar") festlegen, sind Markenanmelder in der Wahl des Darstellungsmittels nicht völlig frei. Im Interesse, Verfahren in Markenangelegenheiten gleichförmig und effizient bearbeiten zu können, geben das DPMA und das EUIPO letztlich verbindliche Vorgaben für die Darstellung der zur Eintragung als Marke angemeldeten Zeichen vor. Für den Bereich des deutschen Markensystems ergeben sich die Vorgaben aus der Markenverordnung sowie einer ergänzenden Bekanntmachung des DPMA, die Vorgaben zu den beim DPMA lesbaren Datenträgertypen, der Datenträgergestaltung und den Formatierungen für Markendarstellungen, einschließlich der zulässigen Dateiformate, enthält.

Ein Blick in die Bekanntmachung zeigt, dass sich die Rahmenbedingungen für den Schutz moderner Markenformen durch die Gesetzesänderung erheblich verbessert haben. Neben der nach wie vor möglichen grafischen Darstellung der Marke auf Papier oder als JPEG-Datei, bestehen nun alternative Darstellungsmittel, die den Markenschutz für bestimmte Markenformen oder einzelner Elemente überhaupt erst praktisch möglich machen. So können Klangmarken nun im Register auch als MP3-Datei gespeichert und wiedergegeben werden, wo bislang lediglich eine Wiedergabe in Notenschrift oder als Sonogramm möglich war. Bewegungsmarken, Multimediamarken und Hologrammmarken können durch Videodateien im MP4-Format wiedergegeben, dreidimensionale Marken in den Dateiformaten OBJ, STL, X3D angemeldet und ins Register eingetragen werden.

„Sonstige Marken" – Der Weg ins Land der unbegrenzten Möglichkeiten?

Trotz des pragmatischen und liberalen Ansatzes, den Gesetzgeber und Ämter im Interesse erfolgreicher Markenanmeldungen verfolgen, sind die zulässigen Darstellungsmittel für die konventionellen und die wichtigsten modernen Marken-



formen (Wortmarken, Bildmarken, dreidimensionale Marken, Farbmarken, Klangmarken, Positionsmarken, Kennfadenmarken, Mustermarken, Bewegungsmarken, Multimediamarken, Hologrammmarken) weitgehend festgelegt. Den praktischen Bedürfnissen der Markenanmelder werden die Vorgaben jedoch gerecht und haben insbesondere die Möglichkeiten, einzelne Merkmale moderner Zeichen besonders in den Vordergrund zu stellen, erheblich erweitert.

Doch damit nicht genug: Eintragungsfähig sind – über die genannten Markenformen hinaus – auch „sonstige Marken", solange sie sich durch ein sachgerechtes Darstellungsmittel (JPEG, MP3, MP4, ggf. textliche Beschreibung, wenn eine Darstellung anders nicht möglich ist) in einer Weise darstellen lassen, die den Anforderungen der klaren und eindeutigen Bestimmbarkeit genügt. Dies eröffnet die Möglichkeit, neue Markenformen einzutragen, die bislang praktisch vom Schutz ausgeschlossen waren. So ermöglicht die Reform des Markenrechts nun auch die Eintragung solcher Marken, die einzelne Aspekte konventioneller und/oder moderner Markenformen kombinieren, etwa in Form einer „Hologrammmustermarke" oder einer „Positionsbewegungsmarke". Darüber hinaus sind aber auch gänzlich neue Markenformen denkbar, so z.B. eine „Lichtmarke", bei der das markenrechtlich geschützte Zeichen in einer bestimmten Form der Ausleuchtung eines Raumes besteht. Möglich sind nun auch konzeptuelle Markenformen, die Markenschutz für bestimmte Merkmale der Raum- oder Umgebungsgestaltung beanspruchen. Dies kann etwa eine 5cm dicke Sandschicht bestimmter Körnung und Farbe auf dem Boden eines Reisebüros oder die Temperierung eines Bademodengeschäfts bei 5 °C sein. Zu beachten bleibt allerdings, dass die weiteren Voraussetzungen des Markenschutzes, vor allem eine Unterscheidungskraft des Zeichens und das Fehlen eines Freihaltebedürfnisses, selbstverständlich auch für die modernen Markenformen gelten.

Der Fantasie von Marketingabteilungen und -agenturen sind damit durch die neuen technischen Möglichkeiten der Darstellung zur Eintragung angemeldeter Marken kaum mehr Grenzen gesetzt. Dies gilt insbesondere für Marken, die an den Seh- und/oder Hörsinn gerichtet sind. Beschränkungen bestehen gleichwohl noch in Fällen, in denen Marken an andere als die genannten Sinne gerichtet sind. Haptische und olfaktorische Reize lassen sich auch mit den nun zulässigen Darstellungsmitteln wohl nicht in einer den Anforderungen des Erfordernisses der klaren und eindeutigen Bestimmbarkeit speichern und wiedergeben. Grundsätzlich ist das Markenrecht jedoch auch für solche Tast- und Geruchsmarken offen – was noch fehlt, ist lediglich eine technische Lösung, mit der die rechtlichen Möglichkeiten ausgeschöpft werden können.

Praxishinweis

Die Spielwiese des Markenrechts ist seit der jüngsten Reform – jedenfalls für Marken, die den Seh- und/oder Hörsinn ansprechen – ein Land der nahezu unbegrenzten Möglichkeiten. Unternehmen bieten sich durch die neuen Darstellungsmöglichkeiten im Register tatsächlich Spielräume für innovative Wege in der Marktkommunikation. Dies gilt insbesondere für solche Unternehmen, die ihre Produkte über digitale

Kanäle vertreiben und bewerben. Stellungnahmen führender Beamter des DPMA lassen eine gewisse Enttäuschung durchblicken, dass Markeninhaber von den neuen Möglichkeiten bislang nur in geringem Umfang Gebrauch gemacht haben.

Nicht übersehen werden darf, dass das Anmelde- und Eintragungsverfahren einige Tücken und Fallen bereithält, die es unbedingt zu umschiffen gilt. Mit der Anmeldung wird die Darstellung der Marke endgültig festgelegt und kann nicht mehr geändert werden. Entsprechend müssen Fehler vermieden werden, die sich im Ergebnis nachteilig auf den beantragten Markenschutz auswirken können und den Wert einer Marke erheblich beeinträchtigen. Wer typische Fehler bei der Anmeldung vermeidet, kann durch den Einsatz moderner Markenformen besondere Aufmerksamkeit erzielen, sich von Konkurrenten absetzen und hierdurch einen spürbaren Vorteil im Wettbewerb erlangen.

Für sämtliche Fragen zum Markenrecht stehen Ihnen gerne zur Verfügung:

Dr. Stefan Maaßen, LL.M.
0221 650 65-231
stefan.maassen@loschelder.de

Dr. Patrick Pommerening
0221 650 65-134
patrick.pommerening@loschelder.de

Mehr als Bitcoin – Blockchain-Technologie in der Vertriebskette

Die Blockchain ist aus den Wirtschaftsnachrichten nicht mehr wegzudenken. Insbesondere in der Finanzwelt haben sich Meldungen rund um Kryptowährungen auf Blockchain-Basis – allen voran Bitcoin – zu einem echten Dauerbrenner entwickelt. Wo die Bitcoin-Reise hingeht, lässt sich nicht seriös vorhersagen. Es ist möglich, dass sich die Begeisterung für Bitcoin als ungerechtfertigter Hype entpuppt – es ist aber auch nicht ausgeschlossen, dass sich eine Kryptowährung tatsächlich einmal zu einem weit verbreiteten Zahlungsmittel entwickelt. Eins ist jedoch klar: Die Technologie hinter Bitcoin hat sich längst emanzipiert. Anwendungen auf Blockchain-Basis können vielfältig eingesetzt werden. Auch wenn die Technologie noch in den Kinderschuhen steckt, wird dem disruptiven Potential der Blockchain nachgesagt, ganze Wirtschaftsbereiche revolutionieren zu können. Dabei muss es nicht immer um neue Geschäftsfelder gehen. Auch im Vertrieb birgt die neue Technologie das Potential für tiefgreifende Veränderungen – selbst beim Vertrieb analoger Güter. Die betroffenen Unternehmen stellt Blockchain in jedem Fall vor neue Herausforderungen – auch rechtlicher Art.

Idee und Technik hinter Blockchain

Bitcoin ist letztlich nur der erste populäre Anwendungsfall einer Technologie, deren Verspechen darin besteht, jede Datentransaktion und jedes in Daten umsetzbares Ereignis verlässlich und fälschungssicher validieren zu können, ohne auf eine zentrale Institution angewiesen zu sein. Anwendungen auf Blockchain-Basis können deswegen grundsätzlich überall dort zum Einsatz kommen, wo es bislang eines vertrauenswürdigen Vermittlers bedarf, der Informationen sicher verwaltet und Transaktionen verifiziert.

Der Begriff „Blockchain“ bezeichnet nicht eine bestimmte Anwendungssoftware oder ein bestimmtes Programm, sondern eine kontinuierlich erweiterbare Liste von Datensätzen („Blöcke“), die mittels kryptografischer Verfahren miteinander verkettet sind. Dies geschieht über einen kryptographisch sicheren Hash (Streuwert), den jeder Block erhält und der auch in jedem neuen Block der Kette zusätzlich zu den neuen Transaktionsdaten enthalten ist. Aus dem Hash des vorangehenden Blocks und den Transaktionsdaten wird ein neuer Hash errechnet, der wie ein Kettenglied als Verbindung zum nachfolgenden Block dient. Welche Voraussetzungen eine Transaktion erfüllen muss, um in einem Block gespeichert und an die Blockchain angehängt zu werden, ist in einem Protokoll festgehalten.

Die Blockchain wird in einer Datenbank parallel und dezentral auf zahlreichen in einem Netzwerk miteinander verbundenen Computern gepflegt. Neue Transaktionen, die die im Blockchain-Protokoll festgelegten Bedingungen erfüllen, werden vom gesamten Netzwerk per Mehrheitskonsens validiert und in allen Dateikopien abgespeichert. Sobald eine Transaktion einmal vom Netzwerk validiert wurde, kann sie im Nachhinein nicht mehr verändert werden. Erfüllt eine Transaktion die Bedingungen nicht, wird die Transaktion

von den Netzwerkteilnehmern abgelehnt. Eine Blockchain lässt sich daher in etwa als dezentrales, allumfassendes und transparentes Kontobuch verstehen, in dem alle Transaktionen zwischen den Netzwerkteilnehmern registriert sind. Kopien des Kontobuchs sind bei jedem einzelnen Teilnehmer hinterlegt und werden parallel fortgeschrieben.

Weil jeder Netzwerkteilnehmer über eine Kopie aller Transaktionsdaten verfügt und auf dieser Grundlage die Validität neuer Transaktionen prüft, bevor er seine Zustimmung erteilt, ist es theoretisch zwar nicht unmöglich, praktisch aber über alle Maßen schwer, die Blockchain zu manipulieren: Um eine Transaktion zu fälschen, genügt es nicht, auf eine Institution einzuwirken – es müssten zeitgleich die Datensätze mindestens der Hälfte der Netzwerkteilnehmer verändert werden, damit eine nicht regelgerechte Transaktion validiert werden kann.

Anwendungsbeispiele für Blockchain im Vertrieb

Die Blockchain-Technologie ermöglicht erstmals Transaktionen unmittelbar zwischen den einzelnen Teilnehmern eines Netzwerks („peer to peer"), ohne dass ein vertrauenswürdiger Intermediär eingeschaltet werden muss. Gerade hierin liegt das Potenzial der Blockchain, bisherige Geschäfts- und Verwaltungsprozesse von Grund auf zu reformieren und auch traditionelle wirtschaftliche Produktions- und Vertriebsketten auf den Kopf zu stellen. Ihr Einsatz in der Vertriebskette kann einerseits mehr Transparenz schaffen, andererseits aber auch Zwischenhändler und Mittelsmänner überflüssig machen.

Die technische Entwicklung der vergangenen Jahre hat neue Formen der Medienproduktion und des Medienkonsums geschaffen. Das Web 2.0 hat nicht nur Katzenvideos zu ungeahnter Popularität verholfen, sondern auch neue Marktteilnehmer hervorgebracht, die den etablierten Akteuren in der Kreativwirtschaft Marktanteile streitig machen. Trotz aller technischer Neuerung hat sich eins bislang nicht geändert: Der Medienvertrieb erfolgt in der Regel zentralisiert. Ob etablierter Künstler oder Star am Blogger-Himmel, Medienschaffende sind bislang auch in der digitalen Welt auf große Plattformbetreiber und Medienkonzerne angewiesen, an die ein Großteil der Einnahmen geht – sei es, wie im Falle von Spotify und Netflix, in Form von Abonnementgebühren, sei es, wie im Falle von Facebook und Google, in Form von Werbeeinnahmen.

Die Möglichkeit, Peer-to-Peer-Transaktionen mittels Anwendungen auf Blockchain-Basis bei geringen Transaktionskosten durchzuführen, kann den Vertrieb von Medien und anderer digitaler Güter auf neue Beine stellen und das Rechtemanagement, die Lizenzvergabe sowie die zugehörigen Abrechnungsmodelle weit mehr revolutionieren, als dies die digitale Transformation bislang getan hat. Blockchain-basierte Geschäftsmodelle ermöglichen es, Nutzungsrechte und Vergütung unmittelbar und direkt zwischen Medienschaffenden und Konsumenten auszutauschen, ohne dass Gelder durch Plattenlabels, Produktionsfirmen oder Vertriebsplattformen laufen müssen.

Denkbare Anwendungsfälle der Blockchain-Technologie in der Vertriebskette sind aber nicht auf digitale Güter beschränkt. Auch in analogen Vertriebsketten kann die Blockchain-Technologie Vertriebswege verkürzen und mehr Transparenz schaffen. Anwendungen auf Blockchain-Basis erlauben es, auch analoge Güter entlang der Vertriebskette zu verfolgen. Hierdurch kann ein echter Mehrwert entstehen, lässt sich doch – bei Einbindung entsprechender Schnittstellen und


PRADA
PRADA

Interfaces auch für Verbraucherinnen und Verbraucher – zurückverfolgen, ob tatsächlich „Bio", „Fair Trade" oder „Made in Germany" drin ist, wo „Bio", „Fair Trade" oder „Made in Germany" draufsteht. Blockchain-Anwendungen in der Vertriebskette können auf diese Weise das Verbrauchervertrauen erhöhen und einen echten Mehrwert für Unternehmen generieren. So meldete der französische Lebensmittelhändler Carrefour, der gemeinsam mit IBM an einer Blockchain-Lösung arbeitet, bereits positive Umsatzentwicklungen beim Verkauf von „Blockchain-Hühnchen" gegenüber den nicht Blockchain-registrierten Alternativen.

Gefährlich kann die Blockchain im Vertrieb hingegen für solche Marktteilnehmer werden, die vor allem Zertifizierungs- und Clearingaufgaben entlang der Vertriebskette übernehmen. Die Möglichkeiten, validierte Informationen und Daten in Blockchain-basierten Datenbanken zu erfassen und den Marktteilnehmern nahezu in Echtzeit zur Verfügung zu stellen, könnte solche Marktteilnehmer schlicht überflüssig machen, sofern sie keinen zusätzlichen Mehrwert bieten.

Die zuverlässige Rückverfolgbarkeit von Gütern bis an ihren Ursprung kann darüber hinaus neue Impulse bei der Durchsetzung, Verteidigung und der Verwaltung von Rechten des geistigen Eigentums liefern, insbesondere bei der Verfolgung von Produktpiraterie oder von Verstößen gegen die Bedingungen eines Vertriebssystems. Auch hier bietet die Blockchain-Technologie neue Möglichkeiten, Herkunft, Vertriebsweg und Echtheit von Markenprodukten über ihren gesamten Lebenszyklus hinweg nachzuvollziehen. Der Luxusgüterhersteller LVMH Moët Hennessy Louis Vuitton, Microsoft und das Softwareunternehmen ConsenSys haben hierfür bereits eine Kooperation zur Entwicklung der Blockchain-Plattform „AURA" geschlossen. AURA soll es den Kunden ermöglichen, die Produkte der Marken der LVMH-Gruppe bis zu ihren Rohmaterialien zurückzuverfolgen und einen Echtheitsnachweis liefern – auch dann, wenn die Waren gebraucht gekauft werden.

Rechtliche Herausforderungen

Auch wenn viele Anwendungsszenarien der Blockchain im Vertrieb (und weit darüber hinaus) technisch umsetzbar sind, stellen gerade die tragenden Grundideen hinter der Technologie das Recht vor größte Herausforderungen. Insbesondere die Unveränderbarkeit von Daten, die einmal in der Blockchain gespeichert sind, lässt sich mit tragenden Prinzipien des Zivilrechts kaum vereinbaren und stellt auch das Datenschutzrecht vor neue Herausforderungen.

So lassen sich die rechtlichen Konsequenzen in der Blockchain nicht abbilden, wenn sich ein Rechtsgeschäft – etwa wegen Anfechtung, Geschäftsunfähigkeit, Sittenwidrigkeit oder eines Verstoßes gegen ein gesetzliches Verbot – als nichtig erweist oder wegen der Beteiligung eines Minderjährigen schwebend unwirksam ist. Transaktionen, die es rechtlich nie gegeben hat, lassen sich in der Blockchain ohne Mitwirkung des Vertragspartners nicht automatisch rückabwickeln, rechtlich vorgesehene Schwebezustände kennt die Blockchain nicht. Datenschutzrechtlich steht die Unveränderbarkeit von Daten in der Blockchain insbesondere der Durchsetzung von Betroffenenrechten entgegen. Wer die datenschutzrechtlich verantwortliche Stelle ist, lässt sich in dezentralen Netzwerken nicht ohne weiteres bestimmen. Auch darüber hinaus wirft der Einsatz der Blockchain-Technologie zahlreiche Rechtsfragen auf, insbesondere in hochregulierten Märkten wie der Finanzbranche oder der Energiewirtschaft.

Die sich hieraus ergebenden (Rechts-)Fragen und Probleme müssen daher in den Nutzungsbedingungen für Blockchain-Anwendungen ausdrücklich thematisiert und angegangen werden. Insoweit wird es dem Einsatz der Blockchain-Technologie helfen, dass die wenigsten der gegenwärtig denkbaren Anwendungsfälle auf die Technologie in ihrer reinsten, nämlich vollständig dezentralisierten Form zurückgreifen werden. Vielmehr wird regelmäßig ein Unternehmen oder ein Konsortium von Unternehmen als Betreiber agieren, das Infrastruktur bereitstellt, konkrete Vorgaben für die Nutzung macht und Nutzungsverträge mit allen Netzwerkteilnehmern schließt. Der Betreiber der Blockchain-Anwendung wird daher häufig Verantwortlicher im Sinne des Datenschutzrechts und gegebenenfalls einschlägiger regulatorischer Vorgaben sein. Darüber hinaus hat er die Möglichkeit, durch die Gestaltung seiner Nutzungsbedingungen auf vertraglicher Grundlage Mechanismen vorzusehen, die bestehende Diskrepanzen zwischen Technik und Recht nach Möglichkeit beseitigen – z.B. durch vertragliche Mitwirkungspflichten bei der Rückabwicklung gescheiterter Transaktionen.

Dass es darüber hinaus in absehbarer Zeit einen geschlossenen gesetzlichen Rechtsrahmen für die Anwendung der Blockchain-Technologie im Wirtschaftsverkehr geben wird, ist unwahrscheinlich. Unternehmen, die mit der Blockchain in Berührung kommen, sei es freiwillig, sei es auf Wunsch eines Geschäftspartners, sollten sich in jedem Fall rechtzeitig über rechtliche Risiken und drohende Fallstricke informieren und umfassend beraten lassen.

Für sämtliche Fragen zu modernen Vertriebsformen stehen Ihnen gerne zur Verfügung:

Dr. Stefan Maaßen, LL.M.
0221 650 65-231
stefan.maassen@loschelder.de

Dr. Patrick Pommerening
0221 650 65-134
patrick.pommerening@loschelder.de


Travel
amazon
Amazon

Datenschutzrecht

Tracking-Tools und digitale Plattformen im Einklang mit EU-Recht: Herausforderungen aus DSGVO, ePrivacy-Recht und P2B-Verordnung

Das Angebot an Marketing-Tools ist kaum überschaubar: Anbieter überbieten sich mit noch treffsichereren Tracking- und Analysetools, um die eigene Werbung genau dort zu platzieren, wo sie zu einer Kaufentscheidung führen wird, oder Digitalnutzer so zu motivieren, dass sie möglichst viel Zeit mit dem vermarkteten Produkt verbringen. Wenn dieses als Plattform für die Vernetzung verschiedener Parteien und den Produkt- oder Dienstleistungsvertrieb in verschiedene Richtungen konzipiert ist, gilt ab Sommer 2020 eine neue EU-Verordnung mit Detailvorgaben für die Vertragsgestaltung. Tracking- und Analysetools werden dagegen von den Aufsichtsbehörden mit besonderer Aufmerksamkeit verfolgt und sollen nach dem Willen einiger bald nur noch mit Einwilligung nutzbar sein. Wann genau welche Regelungen zu beachten sind und ob der plakative Satz „kein Tracking ohne Einwilligung" so wirklich gilt, möchten wir Ihnen nachfolgend erläutern.

Neue Vorgaben für Tracking & Co.

Auf EU-Ebene wird seit einigen Jahren eine Reform des ePrivacy-Rechts diskutiert: Wie die EU-Datenschutzgrundverordnung im Mai 2018 das Datenschutzrecht revolutionierte, sollte eigentlich zur gleichen Zeit die sog. ePrivacy-Verordnung den Bereich der elektronischen Kommunikation entsprechend revolutionieren. Dazu kam es aber mangels Einigung im Rat bis heute nicht – der ePrivacy-Verordnungsentwurf wurde intensiv zwischen den Mitgliedstaaten diskutiert. Nachdem auch der am 8. November 2019 zuletzt unter der finnischen Ratspräsidentschaft veröffentlichte neue Entwurfstext scheiterte, ist die Entscheidung nunmehr gefallen: Die Kommission muss einen neuen Entwurf erarbeiten und vorlegen. Eine zur DSGVO komplementäre ePrivacy-Verordnung ist damit in weite Ferne gerückt.

Damit bleibt es beim Status quo: Es gilt die zuletzt Anfang der 2000er geänderte ePrivacy-Richtlinie, die mit dem technologischen Fortschritt kaum Schritt halten kann und deren Verhältnis – nebst nationalem Umsetzungsrecht – zur DSGVO höchst umstritten ist. Konkret gilt damit auch künftig Art. 5 Abs. 3 der ePrivacy-Richtlinie weiter. Dieser sagt u.a., dass Cookies nur dort ohne Einwilligung des Nutzers gesetzt werden dürfen, wo diese „unbedingt erforderlich" sind, um den gewünschten Dienst zur Verfügung zu stellen. Umgesetzt war diese Regelung nach bisher überwiegender Meinung im deutschen Recht allerdings nicht. Das Telemediengesetz erlaubt nach unbefangener Wortlautlektüre das Setzen der meisten Cookies, solange der Nutzer nicht widerspricht. Womöglich wird der Bundesgerichtshof dies nun – nach dem EuGH-Urteil in Sachen Planet 49 vom 1. Oktober 2010 – richtlinienkonform auslegen; der Vorlagebeschluss deutet dies an. Andern-

falls hat bereits der deutsche Gesetzgeber angekündigt, das TMG nachbessern zu wollen. Aber was bedeutet dies nun für den Einsatz von Tracking-Tools?

Cookies & Co. nur noch unter engen Voraussetzungen

Zunächst einmal eine erhebliche Rechtsunsicherheit: Es ist zunächst noch völlig offen, ob Art. 5 Abs. 3 ePrivacy-Richtlinie überhaupt in Deutschland zur Anwendung kommt. Und selbst wenn dies vom BGH Ende Januar 2020 oder im Nachgang vom Gesetzgeber positiv geklärt würde, bliebe die Frage, was „unbedingt erforderlich" ist.

Gilt das Einwilligungserfordernis aus Art. 5 ePrivacy-Richtlinie, so ist dieses Erfordernis unabhängig von einem etwaigen Personenbezug; anders, als die DSGVO, gilt das ePrivacy-Recht gerade nicht nur für personenbezogene Daten. Art. 5 ePrivacy-Richtlinie gilt vielmehr für alle Informationen, die im Endgerät eines Teilnehmers oder Nutzers gespeichert sind bzw. werden. Entscheidend wird damit in der Praxis die Bestimmung, ob ein Cookie „unbedingt erforderlich" im Sinne der Richtlinie ist. Dies ist, da vom EuGH offen gelassen und auch im Übrigen nicht endgültig definiert, im Einzelfall oftmals nicht eindeutig zu bestimmen; die Debatte darum ist noch im Fluss. Zu einzelnen Cookies lassen sich aber nach Auswertung verschiedener Behördenstellungnahmen eindeutige(re) Aussagen treffen. Wir haben zu Ihrer Orientierung im Folgenden die Cookies in Risikogruppen eingeteilt. Damit können Sie besser abschätzen, ob Ihr Cookie ohne Einwilligung verwendet werden darf bzw. welches Risiko besteht, dass eine Nutzung nur nach vorheriger Einwilligung zulässig ist. Es gilt, wie auch bisher: Im gelben Bereich ist eine umfassende rechtliche und tatsächliche Risikoabwägung erforderlich, im grünen Bereich können Sie Cookies verhältnismäßig rechtssicher auch ohne Einwilligung nutzen und im roten Bereich sollten Sie stets nur nach Einwilligung entsprechende Cookies setzen.

Als erster Indikator zur groben Einschätzung bestehender Risiken ist die folgende Maßgabe hilfreich:

- Sog. Session-Cookies sind mit größerer Wahrscheinlichkeit zulässig als sog. Persistent-Cookies.

- Sog. First Party-Cookies sind mit größerer Wahrscheinlichkeit zulässig als sog. Third Party-Cookies.

„Session-Cookies" sind Cookies, die gelöscht werden, wenn der Nutzer seinen Browser schließt. Cookies, die über eine Browser-Session hinaus gespeichert werden, nennt man „Persistent-Cookies". Durch Letztere können z.B. die Vorlieben oder Aktionen eines Nutzers auf der Webseite oder auch oftmals Webseiten-übergreifend nachvollzogen werden.

Die Unterscheidung „First Party" oder „Third Party" bezieht sich auf die Webseite, die den jeweiligen Cookie platziert. „First Party"-Cookies werden direkt von der Webseite gesetzt, die der Nutzer gerade besucht. Demgegenüber werden „Third Party"-Cookies gerade nicht von dem Webseitenbetreiber, sondern von einem Dritten wie z.B. Google oder Facebook oder von anderen Werbenetzwerken gesetzt. Technisch ist dies möglich, wenn in die Webseite Elemente von Dritten, wie z.B. Social Plugins von Google, Facebook, Twitter etc., eingebunden werden, die von dem Browser des jeweiligen Nutzers beim Aufrufen der Seite ebenfalls geladen werden.


Datenschutz
Allgemein
Tabs
Autom. ausfüllen
Passwörter
Suchen
Sicherheit
Datenschutz
Websites
Erweiterungen
Erweitert
Cookies und Website-Daten:
Immer blockieren
Nur von aktueller Website erlauben
Nur von Websites erlauben, die ich besuche
Immer zulassen
Websitedaten verwalten ...
Website-Tracking:
Tracking durch Websites ablehnen
?

Die Cookie-Ampel

Erklärung der jeweiligen Farben (Einschätzungen jeweils nach aktuellem Diskussionsstand; die rechtliche Bewertung ist indes im Fluss):

- *ohne Einwilligung zulässig*
- *eher ohne Einwilligung zulässig (bei enger, abgesicherter Zweckbindung)*
- *eher nur mit Einwilligung zulässig*
- *nur mit Einwilligung zulässig*

- Für den technischen Betrieb der Webseite erforderliche Cookies
- Cookies, die für die Dauer einer Session notwendig sind, um gewünschte Dienste anzubieten, etwa für die Warenkorbfunktion eines Online-Shops während einer laufenden Session
- Cookies, die für das Ausfüllen einer Maske über mehrere Seiten hinweg notwendig sind und nach Ende der Sitzung (Session) gelöscht werden
- Authentifizierungscookies, die für die Dauer einer Session den Log-in-Status eines Nutzers dokumentieren
- Cookies, die zur Anpassung der Benutzeroberfläche, z.B. Speicherung der Sprachauswahl auf einer internationalen Webseite, notwendig sind
- Nutzerorientierte Sicherheitscookies zur Erkennung von Authentifizierungsmissbrauch für eine begrenzte längere Dauer (Session-Cookie bzw. auf kurze Zeit beschränkter Persistent-Cookie)
- Multimedia-Player-Cookies wie Flash-Player-Cookies für die Dauer einer Sitzung (Session)
- First Party-Cookies zu statistischen Analysezwecken, z.B. zur Messung der Reichweite auf einer einzelnen Webseite (insbesondere wenn die Daten dafür anonymisiert oder zumindest pseudonymisiert werden)
- Third Party-Cookies zu Analysezwecken wie z.B. eTracker; entsprechende Angebote von Google Analytics werden deutlich kritischer gesehen, u.a. wegen der zugrunde liegenden vertraglichen Vereinbarungen.
- First Party Tracking-Cookies, die das Nutzerverhalten über mehrere Webseiten hinweg nachverfolgen
- Sog. Plug-ins Sozialer Netzwerke wie Facebook, Instagram oder Twitter, wenn diese Webseiten-übergreifend Tracking ermöglichen
- Third Party-Cookies für personalisierte Werbung (Webseiten-übergreifendes Tracking und Erstellung von Nutzerprofilen)

Der rechtssicherste Weg (ohne Haftungs- oder Abmahnrisiken) bei der Verwendung von gelb bzw. orange eingestuften Cookies ist weiterhin die Einholung der Einwilligung der Nutzer. Dies entspricht für sämtliche „personenbeziehbare Cookies“ auch der bisherigen Einschätzung der deutschen Aufsichtsbehörden: Etwa der Einsatz von Third Party-Cookies zu Analysezwecken ist nach Ansicht der deutschen Aufsichtsbehörden in vielen Fällen nur mit Einwilligung möglich. In der Praxis finden sich dagegen auch gute Argumente für den Einsatz aus überwiegenden berechtigten Interessen. Eine gerichtliche (höchstrichterliche) Klärung gibt es noch nicht.

Anfang November haben die deutschen Aufsichtsbehörden ihre Position in Bezug auf Google Analytics nochmals bekräftigt: Das Tool sei nur mit Einwilligung rechtmäßig nutzbar. Auf alle Analysetools ist diese Position aber wohl nicht ungeprüft übertragbar, da Google Analytics auch bei Durchsicht der zugrundeliegenden Verträge einige Fragen aufwirft. Verarbeiten oder beinhalten Cookies personenbezogene Daten, können rechtwidrige Cookie-Praktiken zu erheblichen DSGVO-Bußgeldern führen; im ePrivacy-Bereich drohen nach aktuellem Recht zuvörderst zivilrechtliche Abmahnungen.

Anforderungen an eine Einwilligung

Wenn eine Einwilligung erforderlich ist, muss diese den Anforderungen der EU-Datenschutzgrundverordnung genügen. Dies bedeutet insbesondere, dass Einwilligungen aktiv abgefragt werden müssen und nur bei ausreichender, verständlicher Vorab-Information wirksam sein können. Dies bedeutet auch, dass Cookies & Co. zunächst nicht gesetzt werden dürfen, solange vom Nutzer kein aktiver Klick erfolgte.

Über Cookie-Banner kann daher eine wirksame Einwilligung nur eingeholt werden, wenn zumindest folgenden Anforderungen genügt wird:

- Die betreffenden Cookies werden nur und erst gesetzt, nachdem ein Besucher bzw. Nutzer dies durch aktives Klicken bestätigt hat.

- Webseitenbetreiber müssen den Nutzern über das Cookie-Banner die Möglichkeit geben, verschiedene Cookies aktiv anzunehmen. Die oftmals einzig angebotene Möglichkeit, der Nutzung aller Cookies global ohne Differenzierungsmöglichkeiten zuzustimmen, wird den Anforderungen des EuGH zukünftig allenfalls noch gerecht werden, wenn nur ein Typ einwilligungsbedürftiger Cookies verwendet wird, etwa ausschließlich Google Analytics. Um den Anforderungen gerecht zu werden, kann es sich etwa anbieten, dem Nutzer der Webseite die verwendeten Cookies nach der Funktionsweise gruppiert darzustellen und ihn dann aktiv auswählen zu lassen, welche Art von Cookies er zulassen möchte. Dem Nutzer könnte z.B. die Möglichkeit eingeräumt werden, Felder wie „Einverstanden“ oder „Akzeptieren“ – bestenfalls differenziert nach den unterschiedlichen Kategorien von Cookies (mindestens etwa „funktional“, „zur Verbesserung des Nutzungserlebnisses“ oder „Marketingzwecke“, zudem nach dem Urheber der Cookies) – anzuklicken.

- Für den Cookie-Banner sind klare, nicht irreführende Überschriften zu wählen. Die integrierten Links sollten eindeutig den verlinkten Inhalt bezeichnen.

Die Datenschutzerklärung und das Impressum müssen trotz des Banners zugänglich sein.

Vertragsbedingungen auf P2B-Plattformen

Neue EU-Vorgaben gelten zudem ab Sommer 2020 für Betreiber sog. P2B-Plattformen („platform-to-business“). Dies sind solche Plattformen, die gewerbliche Anbieter und Verbraucher zusammenbringen, also Vertragsschlüsse zwischen diesen anbahnen, etwa die Amazon Market Stores. Allerdings gilt die P2B-Verordnung (EU) Nr. 2019/1150 gerade nicht nur für marktstarke Anbieter, sondern – nach dem Prinzip „one size fits all“ – selbst für das kleine Start Up ab dem ersten Betriebstag.

Ziel der P2B-Plattform ist die Reduktion von Diskriminierungspotential, etwa durch die Anzeige von Suchergebnissen, da derartige Plattformen zunehmend als „Gate-Keeper“ zwischen Anbieter und Endkunde stehen. Dazu enthält die Verordnung für alle erfassten Plattformbetreiber bestimmte Vertragsvorgaben, die gewerbliche Händler schützen und von diesen auch entsprechend geltend gemacht werden können, insbesondere:

- Die AGBs von Plattformbetreibern müssen klar und verständlich formuliert und leicht verfügbar sein. Sie müssen u.a. die Gründe benennen, auf Grundlage derer Plattformbetreiber ihren gewerblichen Nutzern kündigen können oder ihre Produkte nicht mehr oder nur eingeschränkt listen dürfen.

- Eine Kündigung muss ggü. dem gewerblichen Nutzer mindestens 30 Tage im Voraus ausgesprochen und begründet werden. Für eine solche Beendigung, aber auch für Einschränkungen oder Aussetzungen der Nutzungsmöglichkeiten, ist ein internes Beschwerdemanagement vorzusehen. Die Frist von mindestens 30 Tagen kann nur in bestimmten Ausnahmefällen unterschritten werden.

- Plattformbetreiber müssen ihre gewerblichen Nutzer mit einer Vorlauffrist von mindestens 15 Tagen informieren. Inwieweit dies womöglich strengeres deutsches AGB-Recht aufgrund des Anwendungsvorrangs von EU-Recht übergeht und damit in Deutschland zu einer Erleichterung für Plattformbetreiber führt, ist noch in der Diskussion.

- Die Anbieter der Produkte müssen für den Verbraucher auf der Plattform klar erkennbar sein. Zu denken ist in diesem Zusammenhang beispielsweise an das einheitliche Design bei Amazon, welches nicht immer auf den ersten Blick erkennen lässt, ob Amazon selbst Verkäufer der angebotenen Waren ist oder nur als Mittler zu gewerblichen Nutzern fungiert.

- Ranking-Kriterien und die Zusammenstellung von Suchergebnissen müssen transparent sein. Deshalb werden die Plattformbetreiber verpflichtet, die wesentlichen Hauptparameter für das Ranking auf der Plattform einschließlich ihrer relativen Gewichtung zu anderen Parametern in ihren AGB anzugeben. Hat eine Online-Suchmaschine ein Delisting oder eine Ranking-Änderung auf Mitteilung eines Dritten hin vorgenommen, ist die Mitteilung des Dritten dem betroffenen Unternehmen zugänglich zu machen.

- Behandeln Plattform-Anbieter Waren oder Dienstleistungen ihrer gewerblichen Nutzer anders als die von ihnen selbst oder von durch sie kontrollierten Unternehmen vertriebene Waren oder Dienstleistungen, so müssen in den AGB die Gründe hierfür erläutert werden. Dasselbe gilt für Online-Suchmaschinen bei der Listung von eigenen Webseiten im Verhältnis zu Webseiten von gewerblichen Nutzern.

- Schränken Plattformanbieter die Möglichkeit ihrer gewerblichen Nutzer ein, ihre Produkte und Dienstleistungen andernorts zu anderen Bedingungen anzubieten, so müssen sie die Gründe hierfür in ihren AGB erläutern. Dies bedeutet: Eine Best-Preis-Verpflichtung wie etwa bei Hotelvermittlungsportalen ist damit – vorbehaltlich ihrer sonstigen (kartell-)rechtlichen Zulässigkeit – weiterhin möglich, es müssen allerdings die Gründe hierfür genannt werden.

Die Durchsetzung der Verordnung obliegt den Mitgliedstaaten. Bereits in der Verordnung angelegt ist die Berechtigung von Organisationen und Verbänden, Verstöße gerichtlich anzugreifen mit dem Ziel, die Nichteinhaltung der P2B-Verordnung zu beenden und diese künftig zu unterlassen.

Durch die P2B-Verordnung ergeben sich damit erweiterte Rechte für gewerbliche Nutzer, zugleich aber auch erhebliche Einschränkungen in der Vertragsgestaltung für Plattformbetreiber, die gerade bei kleineren, neuen Anbietern zu großen Hürden für den Markteinstieg werden können, etwa die lange Kündigungsfrist bei agiler Projektweiterentwicklung. Ob der gewählte Ansatz „one size fits all“ vor diesem Hintergrund glücklich gewählt ist, darf bezweifelt werden. Jedenfalls erleichtert dies die Anwendung der P2B-Verordnung.

Zu allen datenschutzrechtlichen Fragestellungen, auch rund um ePrivacy und P2B, stehen Ihnen gerne zur Verfügung:

Dr. Kristina Schreiber
0221 650 65-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
0221 650 65-200
simon.kohm@loschelder.de

Gesellschaftsrecht

Digitalisierung im Gesellschaftsrecht – Anforderungen an die Unternehmensführung in Zeiten der Digitalisierung

Die Digitalisierung beeinflusst durch das allgegenwärtige Streben nach Datenerhebung und Datenverarbeitung auch das Gesellschaftsrecht. Aus praktischer Sicht sind dabei insbesondere die Auswirkungen auf eine digitale Unternehmensleitung von Relevanz.

1. Ausgangslage

Unternehmen setzen bereits gegenwärtig unterschiedlichste Formen von Big Data und künstlicher Intelligenz ein. Die Wortschöpfung Big Data wird dabei oft als Sammelbegriff für die moderne digitale Technologie verwendet. Im Wesentlichen beschreibt der Begriff die technische Möglichkeit von Speichermedien und Prozessoren, größte Datenmengen in kürzester Zeit zu verarbeiten, zu verwerten und zu analysieren. So ist es problemlos möglich, ein Computerprogramm über zahlreiche Schnittstellen für verschiedenste Folgeaktionen hinweg autonom arbeiten zu lassen, ohne dass ein Mensch als Mittler auftreten muss. Dieser Fortschritt wird wesentlich durch autonome Algorithmen geprägt, die aufgrund vorgegebener Daten selbstständig handeln und durch jeden getätigten Prozess weiter lernen. Dies wird häufig als Einsatz von künstlicher Intelligenz – kurz KI – bezeichnet. Bekannte Einsatzgebiete derartiger KI-Algorithmen sind autonom gesteuerte Fahrzeuge oder Erkennungssoftware im öffentlichen Raum.

2. Digitale Geschäftsführung

Inwieweit derartige Technik auch im Rahmen der klassischen Unternehmensführung eingesetzt werden sollte oder vielleicht sogar muss, ist derzeit Gegenstand intensiver Diskussionen. Dabei ist zunächst zu berücksichtigen, dass sich die Effizienz der Unternehmensführung vor dem Hintergrund des erreichten technischen Stands insbesondere durch den Einsatz von Big Data und passender Algorithmen durch KI erheblich steigern lassen.

2.1. Eigenständige Unternehmensleitung durch KI

Wenngleich autonome Algorithmen darauf ausgelegt sind, Entscheidungen – ähnlich wie bei autonomen Fahrzeugen – nicht nur unterstützend, sondern eigenständig zu treffen, ist die Ernennung von KI zu Geschäftsleitern jedenfalls im deutschen (Kapital-)Gesellschaftsrecht nach aktueller Gesetzeslage von vorneherein ausgeschlossen, da einzig natürliche, unbeschränkt geschäftsfähige Personen Geschäftsführer bzw. Vorstandsmitglieder von Unternehmen sein

können. Die eigenständige Unternehmensleitung durch KI ist daher nach aktuellem Stand nicht möglich.

2.2. Geschäftsleitung unter Zuhilfenahme von KI

Zulässig und sinnvoll ist hingegen die Unterstützung der (menschlichen) Geschäftsleitung durch den Einsatz von Big Data und KI. Es ist schon heute nicht ungewöhnlich, dass unternehmerische Leitungsentscheidungen zunehmend unter Beteiligung von Big Data, KI und den zugehörigen Computeralgorithmen vorbereitet und getroffen werden.

a) Einsatz von Big Data und KI im Rahmen der Business Judgement Rule (BJR)

Rechtlicher Hintergrund dafür ist insbesondere die BJR, an deren Vorgaben sich Geschäftsleiter von Kapitalgesellschaften zur Verringerung ihres Haftungsrisikos orientieren sollten. Für die BJR ist es von zentraler Bedeutung, dass die Geschäftsleitung unternehmerische Entscheidungen auf der Grundlage angemessener Informationen trifft. Eine angemessene Informationsgrundlage setzt dabei das der Situation angemessene, möglichst umfassende Ausschöpfen von Informationsquellen und deren Einbeziehung in den Entscheidungsprozess voraus.

Für die Schaffung der Informationsgrundlage drängt sich der Einsatz von Big Data zur Sammlung der für die Entscheidung relevanten Daten und deren ggf. KI-gestützter Auswertung geradezu auf. Da die Technik dem Menschen im Hinblick auf das Sammeln von Daten und deren Auswertung in vielen Belangen deutlich überlegen ist, ist der Einsatz von Algorithmen sowohl im Rahmen der Informationsgewinnung durch die Abfrage diverser Datenblöcke aus verschiedensten Datenquellen, als auch im Hinblick auf die Analyse und Ergebnisfindung einer unternehmerisch vernünftigen Entscheidung prädestiniert. Im besten Fall kann durch den Einsatz der Technik auf eine mühselige Datenrecherche und anschließende Auswertung durch (menschliche) Mitarbeiter gänzlich verzichtet werden. Auch eine Entscheidungstendenz kann problemlos vorgeschlagen werden, um die Effizienz der Entscheidungsfindung weiter zu erhöhen.

Zudem lassen sich Entscheidungen durch den Einsatz von KI verobjektivieren, indem sie den Einfluss von Eigeninteressen der Geschäftsleitung auf die Entscheidung verringern. Dies ist vor dem Hintergrund der BJR insoweit relevant, als die BJR Entscheidungen verlangt, die ohne Einfluss von Interessenskonflikten getroffen werden. Da KI – anders als der Mensch – keine Eigeninteressen kennt, kann sie insoweit auch keinen Interessenskonflikten unterliegen. Der Einsatz von KI kann somit auch in dieser Hinsicht helfen, die Voraussetzungen der BJR einzuhalten und das Haftungsrisiko für die Geschäftsleitung zu verringern.

b) Delegation von Aufgaben

Darüber hinaus ist es grundsätzlich zulässig, einzelne Aufgaben auf KI zu delegieren und Algorithmen weitgehend selbständige Entscheidungen treffen zu lassen. Überall dort, wo keine zwingende originäre Leitungsaufgabe vorliegt, können Aufgaben nämlich grundsätzlich delegiert werden, da die Leitung eines Unternehmens ohne Delegation schlichtweg nicht möglich wäre. Soweit die abschließende Entscheidung weiterhin dem Geschäftsleiter obliegt, darf auch moderne Technik eingesetzt werden. Entscheidend ist, dass die Wirkungsweise des Algorithmus‘ bekannt ist und ggf. korrigiert werden kann, wenn Fehler auftreten sollten.

c) Keine Pflicht zum Einsatz von Big Data und KI

Trotz dieser Vorteile besteht derzeit (noch) keine Pflicht für den Einsatz von Big Data und KI bei der Vorbereitung und dem Treffen von unternehmerischen Entscheidungen. Vielmehr dürfen Geschäftsleiter Kosten und Nutzen der Informationsbeschaffung und Entscheidungsfindung in der konkreten Entscheidungssituation gegeneinander abwägen. Gerade in der jetzigen Frühphase des Einsatzes von KI in Unternehmen sind technisch ausgereifte Algorithmen in der Anschaffung und Unterhaltung sehr teuer. Insbesondere für Unternehmen aus dem Mittelstand übersteigen die Kosten von Algorithmen häufig noch deren Nutzen. Je erschwinglicher und treffsicherer Algorithmen jedoch werden, desto weniger wird sich der Verzicht auf technische Unterstützung bei der Entscheidungsfindung rechtfertigen lassen. Letztlich dürfte es nur eine Frage der Zeit sein, bis sich in Zeiten von Big Data und KI eine (kapital-)gesellschaftsrechtliche Pflicht zum angemessenen Einsatz von Algorithmen herausbildet.

3. Fazit

Die Digitalisierung ermöglicht weitreichende Chancen im Rahmen der Geschäftsführung. Die richtige Implementierung intelligenter Algorithmen kann zu einer effizienten und risikominimierten Geschäftsleitung führen. Insbesondere im Rahmen der täglichen Entscheidungsfindung sollten Big Data und KI vor dem Hintergrund der BJR frühzeitig in das Unternehmen eingeführt werden, um sich zeitnah an den Einsatz zu gewöhnen. Nach derzeitiger Rechtslage ist der Einsatz von Algorithmen zwar noch nicht verpflichtend, es ist aber davon auszugehen, dass sich dies in Zukunft ändern wird.

Zu allen Fragestellungen rund um Digitalisierung und Compliance steht Ihnen gerne zur Verfügung:

Dr. Felix Ebbinghaus, LL.M.
0221 650 65-224
felix.ebbinghaus@loschelder.de


RULES AND
REGULATIONS
CLICK

Digitalisierung und Compliance: Welche Strukturen helfen im Unternehmen?

Mit fortschreitender Digitalisierung verändert sich auch das Anforderungsprofil an ein wirkungsvolles Compliance-Management im Unternehmen. Dies zum einen, da neue digitale Prozesse und datenschutzrechtliches Gesetzgebungsfieber neue Herausforderungen mit sich bringen, etwa mit Blick auf digitale Angriffspunkte oder umfangreichere Rechenschaftspflichten. Zum anderen bringt die digitale Transformation aber neue Möglichkeiten des Compliance-Managements mit sich: Vermehrt werden intelligente Systeme eingesetzt, um Arbeitsabläufe zu optimieren, die Aufdeckungsrate zu erhöhen und Risiken frühzeitig zu erkennen.

Digitalisierung führt zu verlagerten Compliance-Pflichten

Ein wesentliches Haftungsrisiko der Geschäftsleitung ergibt sich aus ihrer Compliance-Pflicht. Darunter wird die Pflicht der Geschäftsleitung verstanden, sich nicht nur selbst rechtstreu zu verhalten, sondern auch dafür Sorge zu tragen, dass das von ihnen geleitete Unternehmen und dessen Mitarbeiter keine Rechtsverstöße begehen. Sämtliche Maßnahmen, die ein Unternehmen zur Einhaltung der Regeln sowie zur Vermeidung von Regelverstößen einsetzt, werden als Compliance-Management-System bezeichnet. Compliance-Management-Systeme sind stets auf das jeweilige Unternehmen maßgeschneidert und müssen permanent weiterentwickelt werden, um dem sich wandelnden Unternehmen und sich ändernden regulatorischen Vorgaben anzupassen sowie Prozesse und Abläufe zu optimieren.

Steigt die Digitalisierungsrate im Unternehmen, sollte sich dies denn auch im Compliance-Management spiegeln: neue Anwendungen und IT-Prozesse bringen zugleich andere Anforderungen an das Monitoring mit einem wirkungsvollen „Plan-Do-Check-Act-Zyklus“ mit sich sowie neue Angriffspunkte etwa für Cyber-Attacken. Dies erfordert im Compliance-Management eine entsprechende Priorisierung und Ressourcenbereitstellung. Datenschutz und IT sind im Lichte fortschreitender Digitalisierung und datenschutzrechtlicher Anforderungen Kernthemen einer modernen Compliance-Organisation. Dabei sind beide Bereiche nicht deckungsgleich, erfahrungsgemäß aber an vielen Stellen verzahnt: So bringen neue digitale Anwendungen regelmäßig neue Datenverarbeitungsprozesse (auch personenbezogener Daten) mit sich, die datenschutzrechtskonform abzubilden sind. Spiegelbildlich ist ein wirksamer Datenschutz nicht ohne ein risikoangemessenes Schutzniveau zu gewährleisten: Datenschutz durch Technikgestaltung ist ein zentrales Element der EU-Datenschutzgrundverordnung (DSGVO), ergänzt durch das Erfordernis eines risikoangemessenen IT-Sicherheitsniveaus für die Verarbeitung personenbezogener Daten. Im Unternehmen ist es dann oft sinnvoll, die prozessuale Gestaltung nicht auf den Bereich der personenbezogenen Daten zu beschränken, sondern dies zugleich auf den IT-Bereich insgesamt auszuweiten. Dabei kann dann sogleich geprüft werden, ob der Einsatz intelligenter Systeme mit der Digitalisierung auch der Compliance-Prozesse selbst einen Mehrwert bietet.

Optimierte IT- und Datenschutz-Management-Prozesse

Spätestens mit Inkrafttreten der DSGVO im Mai 2018 ist ein wirkungsvolles Datenschutz-Management unverzichtbar: Nur durch entsprechende Prozessvorgaben kann abgesichert werden, dass

den umfangreichen Rechenschaftspflichten für verantwortliche Stellen bei der Verarbeitung personenbezogener Daten genügt wird (Art. 5 Abs. 2 DSGVO), bei der Datenverarbeitung stets „geeignete technische und organisatorische Maßnahmen“ angelegt sind (Art. 25 DSGVO) sowie ein dem Risiko angemessenes und durch „geeignete technische und organisatorische Maßnahmen“ abgesichertes Datensicherheitsniveau gewährleistet ist (Art. 32 DSGVO). Mit letzterem eng verknüpft und mit fortschreitender Digitalisierung immer wichtiger ist ein entsprechendes IT-Management-System, welches sicherstellt, dass sämtliche digitale Prozesse auch künftig verlässlich, sicher und optimiert gestaltet werden.

Wesentliche Elemente eines Datenschutz-/IT-Managements sind zum einen der Aufbau einer entsprechenden Organisation in subjektiver Hinsicht und zum anderen die – objektive – Festlegung von Leitlinien und Richtlinien für die zentralen Prozesse in den jeweiligen Bereichen:

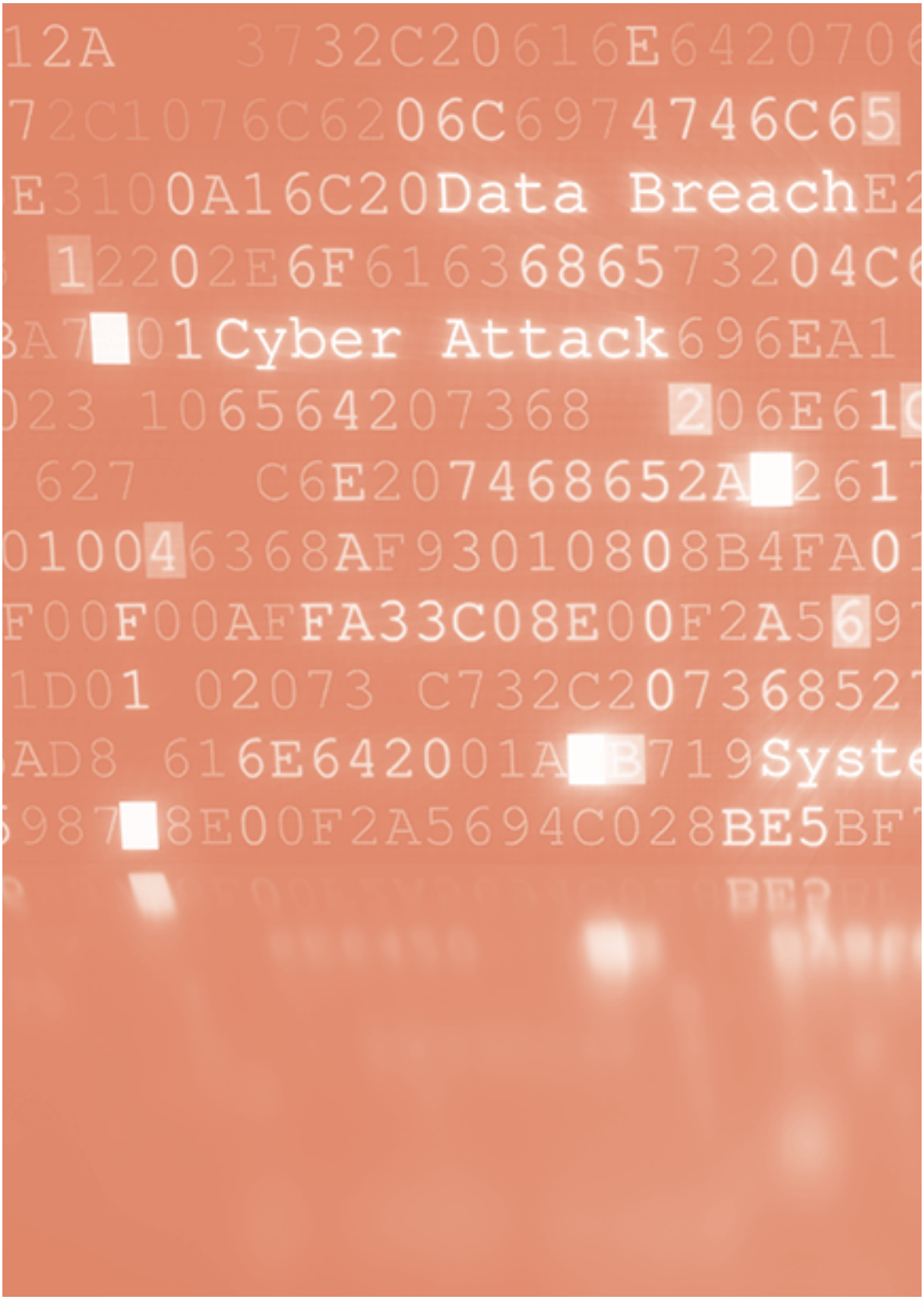
- Organisatorisch liegt etwa nach der DSGVO die gesamte Verantwortung bei der Geschäftsleitung. Diese kann sich durch organisatorische Maßnahmen effektiv entlasten, was angesichts der enormen Aufgaben, die der Datenschutz an Unternehmen stellt, für einen effektiven Datenschutz ohnehin in den meisten Unternehmensstrukturen unverzichtbar ist.

  Ab einer gewissen Unternehmensgröße erfordert dies notwendigerweise mehrere zuständige Personen: Der Datenschutzbeauftragte etwa kontrolliert und informiert, während der Datenschutzkoordinator im Unternehmen zentrale Anlaufstelle auch im Bereich der operativen Umsetzung neuer Prozesse ist. Hierbei kann und sollte der Datenschutzbeauftragte begleiten, er kann aber keine Gestaltungsideen entwickeln und umsetzen: Der Datenschutzbeauftragte ist zentrale Kontrollstelle – was er selbst geschaffen hat, wird er aber nicht wirksam kontrollieren können.

  Neben Datenschutzkoordinator und Datenschutzbeauftragtem sollte es je nach Unternehmensstruktur weitere Datenschutzansprechpartner in den einzelnen Unternehmensbereichen geben, die mit dem Datenschutzkoordinator zusammenarbeiten und ihm etwa Spezialwissen aus ihrem operativen Bereich vermitteln. Schließlich ist auch die Geschäftsführung weiterhin einzubinden. An sie berichten Datenschutzbeauftragter und Datenschutzkoordinator, sie trifft die zentralen Entscheidungen und ihr obliegt die Gesamtsteuerung.

  Gemeinsam bilden alle vorgenannten Personen das „Datenschutzteam“, welches sich regelmäßig über den aktuellen Stand im Unternehmen austauschen und notwendige Verbesserungen diskutieren und umsetzen sollte – als personelle Komponente des „Plan-Do-Check-Act-Zyklus“. Wie meist bietet es sich dabei an, die Team-Bildung an im Unternehmen bekannte und etablierte Strukturen anzulehnen, z.B. aus dem Qualitätsmanagement.

- Die wesentlichen Prozessvorgaben im Datenschutz- wie IT-Bereich sind sodann in entsprechenden Leitlinien und Richtlinien darzulegen und verbindlich an die (jeweils betroffenen) Mitarbeiter auszugeben. Dies umfasst etwa Richtlinien mit Verhaltensvorgaben inhaltlicher Art oder auch Vorgaben für die Reaktion in bestimmten Situationen: Eine Datenpanne – also eine Verletzung des Schutzes personenbezogener Daten, wie sie z.B. durch den Verlust eines Datenträgers oder einen Hacking-Angriff eintreten kann – muss binnen 72 Stunden der Aufsichtsbehörde gemeldet werden. Dies wird sicher nur dann gelingen, wenn alle Mitarbeiter Zugang


12A 3732C20616E6420706
72C1076C6206C6974746C65
E3100A16C20Data BreachE2
1220 2E6F6163686573204C6
3A701Cyber Attack696EA1
023 10656420736 8 206E61C
627 C6E207468652A 2617
0100463 68AF9301080 8B4FA01
F00F00AFFA33C08E00F2A5697
1D01 02073 C732C207368527
AD8 616E64201A B719Syste
5987 8E00F2A5694C028BE5BF7

zu einer entsprechenden Richtlinie haben, die ihnen auch im Fall eines Systemausfalls als „worst case“ noch zur Verfügung steht. Minimal muss die Richtlinie die Mitarbeiter befähigen, eine Datenpanne zu erkennen, und ihnen vermitteln, wen sie in diesem Fall mit welcher Geschwindigkeit und welchen Informationen informieren müssen. Die genaue Ausgestaltung einer solchen Richtlinie erfolgt sinnvollerweise unternehmensindividuell – sie muss die Mitarbeiter auch erreichen und so gefasst sein, dass eine Integration in den Arbeitsalltag gewährleistet ist.

Von grundlegender Bedeutung sind in diesem Kontext auch Notfallpläne: Wie wird etwa im Fall eines Cyber-Angriffs reagiert, welche Mitarbeiter (zuvörderst aus dem IT-Bereich) oder welche externen Dienstleister sind wann erreichbar, um einen 24/7-Support abzusichern? Wer entscheidet über die Einleitung von Sofortmaßnahmen und wie wird abgesichert, dass auch in solchen Fällen hinreichende Backups u.ä. verfügbar sind und die Produktion nicht stillsteht?

Begleitet werden muss dies u.a. durch eine

- hinreichende Dokumentation,
- aktuelle und hilfreiche Wissensvermittlung an die betroffenen Mitarbeiter, jeweils angepasst an den Aufgaben- und Einsatzbereich, sowie
- erfolgreiche Motivation, dass die etablierten Prozesse auch im Alltag gelebt werden.

Sind derartige Prozesse dem Grunde nach etabliert und werden sie gelebt, so sind auch Erweiterungen mit weniger Aufwand möglich – man denke etwa, je nach Unternehmensphilosophie, an den Aufbau einer „Corporate Digital Responsibility“ für eine auch „ethisch“ korrekte Datenwirtschaft oder die Begleitung des Einsatzes künstlicher Intelligenz im Unternehmen, die angesichts der Entwicklung eigener, „intelligenter“ Entscheidungsfindungen noch deutlich weiterreichende Herausforderungen an ihre Flankierung mit sich bringt, als ein reines „Machine Learning“ („maschinelles Lernen“).

Einsatz von KI im Rahmen des Compliance-Managements

Compliance-Organisationen laufen der Weiterentwicklung der regulatorischen Anforderungen und auch der Aufdeckung von Verstößen gegen Gesetze, Regularien oder interne operationelle Produktionsvorgaben bisweilen regelrecht hinterher. An dieser Stelle kann die Digitalisierung eine große Unterstützung bieten durch digitale Compliance-Systeme:

Bei einem umfassenden Einsatz von Big Data ist es z.B. problemlos möglich, zahlreiche Lieferanten oder Konzernunternehmen zeitgleich und in Echtzeit zu überwachen. Algorithmen werten den elektronischen Kommunikationverkehr zunächst verschlüsselt und anonymisiert aus und können scheinbar Fernliegendes in Zusammenhang bringen. Dies ermöglicht es, betrügerisches Handeln durch Mitarbeiter anhand forensischer Datenanalyse innerhalb kurzer Zeit aufzudecken. Dabei werden bei Einsatz weit entwickelter, künstlich intelligenter Systeme Schwachstellen durch den selbstlernenden Algorithmus automatisch gemeldet. Darüber hinaus können vorhersagende analytische Algorithmen mögliche Verstöße bereits frühzeitig erkennen, da sie Verhaltensmuster erkennen und nachverfolgen.

Insbesondere durch den Fortschritt analytischer Systeme ist es möglich, Compliance-Management-Systeme künftig als vorbeugende Instanz einzusetzen. Idealerweise können auf diese Weise Rechtsverstöße verhindert werden, bevor sie entstehen, so dass imageschädigende und wirtschaftlich belastende staatliche Sanktionen von vornherein ausgeschlossen sind.

Doch auch vorgelagert, jenseits der weit entwickelten künstlich intelligenten Compliance-Systeme, bringt die Digitalisierung Unterstützungsmöglichkeiten im Compliance-Bereich, so etwa durch die Strukturierung von Datensätzen, z.B. der automatisierten Belegauswertung, für die oftmals Instrumente mit maschinellen Lernmöglichkeiten ausreichend sind. Digitale Anwendungen können auch durch ein regelmäßiges Monitoring unterstützen, relevante Änderungen der regulatorischen Anforderungen zu erkennen und Umsetzungshilfen zu bieten – derartige Anwendungen werden etwa im Finanzsektor mit umfangreichen regulatorischen Herausforderungen erprobt. Meldefristen können durch entsprechende Anwendungen strukturiert werden, automatisierte Löschprozesse helfen bei der Einhaltung der datenschutzrechtlichen Anforderungen.

Die Digitalisierung bringt damit auch für die Compliance-Abteilung Unterstützung, derzeit noch kaum „von der Stange“, so dass zumeist unternehmensindividuelle Lösungen gefunden werden müssen. Dies aber dürfte der Compliance-Abteilung ohnehin bekannt sein.

Zu allen Fragestellungen rund um Digitalisierung und Compliance stehen Ihnen gerne zur Verfügung:

Dr. Kristina Schreiber
0221 650 65-337
kristina.schreiber@loschelder.de

Dr. Felix Ebbinghaus, LL.M.
0221 650 65-224
felix.ebbinghaus@loschelder.de

Dr. Simon Kohm
0221 650 65-200
simon.kohm@loschelder.de


BUßGELDBESCHEID

Datenschutzrecht

Haftung für Datenschutzverstöße

Eineinhalb Jahre nach Inkrafttreten der DSGVO geht nun doch das Bußgeldgespenst um. Laut vieler Meldungen werden die Datenschutzbehörden aktiver und verhängen teils empfindliche Bußgelder im hohen sieben- bzw. achtstelligen Bereich. Grund genug, sich mit den Grundsätzen der datenschutzrechtlichen Bußgeldhaftung und der aktuellen Behördenpraxis auseinanderzusetzen.

Wer haftet ...

Die DSGVO adressiert ihre Rechtspflichten und damit auch die Konsequenzen bei deren Missachtung an die Verantwortlichen. Zur Erinnerung: Verantwortlich ist, wer über den Zweck und die Mittel der Datenverarbeitung entscheidet (Art. 4 Nr. 7 DSGVO).

Damit ist klar, dass im nicht-öffentlichen Bereich jedenfalls die Unternehmen haften, die eine Datenverarbeitung zu wirtschaftlichen Zwecken eigenverantwortlich durchführen, also bspw. Newsletter versenden, Kundenprofile erstellen oder ihre Mitarbeiter überwachen. Das entspricht dem datenschutzrechtlichen Verständnis einer Unternehmenshaftung, was sich bereits daran zeigt, dass für die Bußgeldberechnung auf den Unternehmensumsatz abgestellt werden soll.

Spannender ist die Frage, ob neben dem Unternehmen auch die natürlichen Personen haften, die den Datenschutzverstoß herbeigeführt oder jedenfalls zu verantworten haben, also beispielsweise ein Angestellter, der Abteilungsleiter oder Mitglieder der Geschäftsleitung (Vorstände, Geschäftsführer). In der juristischen Diskussion wird diese Frage derzeit unterschiedlich beantwortet. Grund dafür ist, dass die DSGVO nur eine Unternehmenshaftung vorsieht, das deutsche Bußgeldrecht hingegen zunächst von einer Haftung natürlicher Personen und hier der (ggf. erweiterten) Geschäftsleitung ausgeht. In der Praxis ist die Frage nach der persönlichen Haftung bisher unbeantwortet geblieben, da die Behörden – soweit ersichtlich – noch keine Bußgelder gegen natürliche Personen verhängt haben.

Problematisch ist die Haftung weiterhin für die Stellen, bei denen umstritten ist, ob sie im datenschutzrechtlichen Sinne verantwortlich sind, also beispielsweise den Betriebsrat.

... wie hoch?

Die Höhe des Bußgeldes galt lange Zeit als Blackbox. Einzig bekannt waren die in der DSGVO genannten Obergrenzen (2% bzw. 4% des Umsatzes der Unternehmensgruppe). Das führte naturgemäß zu wilden Spekulationen und Horrorszenarien. Der Nebel der Unsicherheit hat sich mit dem kürzlich veröffentlichten Datenschutzkonzept der deutschen Aufsichtsbehörden zum Teil gelichtet. In diesem für Gerichte und einzelne Behörden unverbindlichen Dokument haben die Behörden erläutert, wie die mehrschrittige Berechnung eines datenschutzrechtlichen Bußgeldes künftig aussehen kann. Vereinfach lässt sich dazu Folgendes sagen:

- Umsatzermittlung: Zunächst wird der Jahresumsatz der Unternehmensgruppe bestimmt, welcher der Verantwortliche angehört. Ganz wichtig: Es kommt dabei auf den Umsatz der gesamten Unternehmensgruppe an und nicht nur des Verantwortlichen. Eingerechnet werden also auch Umsätze beherrschter und beherrschender Unternehmen.

- Eingruppierung: Sodann erfolgt eine Eingruppierung als „Kleinstunternehmen“, „kleines“, „mittleres“ oder „großes“ Unternehmen anhand eines Rasters, das auf den Umsatz abstellt.

- Bestimmung des Grundwertes: Sodann wird auf der Grundlage von Durchschnittswerten ein sog. Grundwert besimmt, der einen Tagessatz in Euro darstellt. Zu beachten ist, dass bis zu diesem Schritt die Schwere der Tat noch keine Rolle spielt. Es ist also möglich, für jedes Unternehmen den wirtschaftlichen Grundwert und damit das ganz abstrakte Bußgeldrisiko zu ermitteln. Je nach Eingruppierung beträgt dieser Wert 972 EUR für Unternehmen mit 350.000 EUR Umsatz und bis zu 1,25 Mio EUR für Unternehmen bis 450 Mio. EUR Umstatz. Ab einem Umsatz von 500 Mio. EUR wird ein konkreter Tagessatz gebildet.

- Multplikation: Der Grundwert wird sodann mit einem Faktor multipliziert, der sich nach den Tatumständen richtet. Das Bußgeldkonzept geht von folgenden Schweregraden aus: Leicht, mittel, schwer, sehr schwer. Zudem wird unterschieden zwischen formellen und materiellen Verstößen. Entscheidend sind ferner alle sonstigen Umstände, u.a. ob vorsätzlich oder fahrlässig gehandelt wurde, welche Risiken für die Betroffenen bestehen, ob ein Verstoß zum wiederholten Male aufgetreten ist, inwiefern mit der Behörde kooperiert wurde etc. Letztlich wird die Behörde hier immer eine ermessensbasierte Gesamtabwägung treffen.

- Korrektur: Schließlich halten sich die Behörden noch eine Hintertür offen und können das Bußgeld (nach oben und unten) anpassen, wenn insbesondere täterbezogene Umstände dies verlangen.

Der Vorteil des Bußgeldkonzepts liegt also für Unternehmen maßgeblich darin, das abstrakte Ausgangsrisiko (ohne Bewertung einer konkreten Tat) bewerten zu können. Wie die Behörden dann jedoch eine Gesamtabwägung vornehmen, dürfte weiterhin schwer zu prognostizieren sein.

Bisherige Praxis

Die Bußgeldpraxis der Behörden ist noch durch ihre Überlastung geprägt. Behörden müssen bei der Verfolgung von Verstößen ihr Aufgreifermessen ausüben, sich also entscheiden, in welchen Fällen ein Verfahren eröffnet wird. Folgende Verstöße werden in einem auffälligen Maße verfolgt:

- Verstöße im Zusammenhang mit sensiblen Daten, insbesondere Gesundheitsdaten
- Vorsätzliche Verstöße
- Materielle Verstöße im Gegensatz zu rein formellen Verstößen
- Verstöße mit schweren Folgen für die Betroffenen

Erstaunlich ist, dass bisher noch keine Bußgeldfälle im Bereich des Beschäftigtendatenschutzes bekannt geworden sind.

Eine echte und verlässliche Systematik lässt sich hier allerdings noch nicht ableiten. Dafür ist die kritische Masse an Verfahren noch nicht erreicht und auch das Bußgeldkonzept noch zu frisch. Wir beobachten die Entwicklungen für Sie und halten Sie auf dem Laufenden.

Kooperation mit den Behörden

Werden Datenschutzverstöße im Unternehmen bekannt, sind diese bereits an die Behörde gelangt oder hat diese schon ein Verfahren eröffnet, stellt sich stets die Frage, ob und inwieweit mit der Behörde kooperiert werden soll.

Zunächst sieht das Datenschutzrecht keine Möglichkeit einer Selbstanzeige vor. In anderen Rechtsbereichen wie dem Kartell- oder Steuerrecht gibt es solche Mechanismen, die Betroffenen die Möglichkeit eines Straferlasses oder einer Strafmilderung zubilligen, wenn diese Verstöße zugeben und aktiv an die Behörden melden. Nicht nur, dass das Datenschutzrecht keine derartige Möglichkeit eröffnet, schlimmer noch: Die DSGVO verpflichtet Unternehmen, Verstöße ab einer bestimmten Schwelle aktiv an die Behörde (und die Betroffenen) zu melden. Unterbleibt dies, stellt das für sich genommen schon eine bußgeldbewehrte Ordnungswidrigkeit dar. In vielen Fällen haben Unternehmen also gar keine Möglichkeit, über das Ob und Wie einer Kooperation vertieft und lange nachzudenken, da das Gesetz eine schnelle Reaktion erfordert. Entscheidend ist hier die genaue Prüfung der Risiken für die von der Datenpanne Betroffenen. Existieren diese nicht oder sind diese nur sehr gering, kann ggf. auf eine Behördenmeldung und Betroffenenmeldung verzichtet werden.

Im Übrigen wird eine Kooperation mit den Behörden immer bußgeldmildernd sein. Über den Umfang muss im Einzelfall entschieden werden, auch und gerade unter Berücksichtigung der Schwere der Vorwürfe und deren Begründetheit.

Für sämtliche Fragen zum Datenschutzrecht stehen Ihnen gerne zur Verfügung:

Dr. Kristina Schreiber
0221 650 65-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
0221 650 65-200
simon.kohm@loschelder.de


tab
caps lock
shift
fn

Know-how-Schutz

Schutz von Know-how in der digitalen Welt

Die Digitalisierung stellt den Schutz von Betriebs- und Geschäftsgeheimnissen seit Jahren vor wachsende Herausforderungen. Mit dem Inkrafttreten des Geschäftsgeheimnisgesetzes im April 2019 werden diese Herausforderungen noch durch neue rechtliche Vorgaben verstärkt, welche den Schutz von Know-how neu regeln und von geänderten Vorgaben abhängig machen.

Steigende Verwundbarkeit

Es ist bekannt, dass die Gefahr eines unbeabsichtigten Verlustes von Know-how durch die Digitalisierung erheblich zunimmt. Auch wichtige Geheimnisse werden nicht mehr im Tresor des Unternehmens verwahrt, sondern in elektronischer Form auf Servern und in Datenbanken gespeichert. Diese sind regelmäßig in eine IT-Infrastruktur eingebunden, die für die Mitarbeiter und in der Regel auch von außen zugänglich ist. Dies erhöht die Verwundbarkeit für Angriffe von außen und innen in erheblichem Umfang.

Statistiken über Gerichtsverfahren und die Berichte von BND und Verfassungsschutz zeigen, dass die Angriffe auf das Know-how deutscher Unternehmen und die auf diesem Weg verursachten Schäden seit Jahren steigen. Neben professionell ausgeführten Angriffen durch fremde Nachrichtendienste und Wirtschaftsspione zeigen die Statistiken allerdings auch, dass die mit Abstand größte Zahl von Angriffen durch eigene Mitarbeiter erfolgt. Eine Studie aus den USA gelangt nach Analyse von Gerichtsverfahren wegen unberechtigter Know-how-Verwertung zu dem Ergebnis, dass rund 77 % der Verwertungshandlungen von aktuellen oder ehemaligen Mitarbeitern des Unternehmens begangen wurden. Die Situation dürfte in Deutschland, wie auch die Erfahrung zeigt, nicht anders sein. Diese Erkenntnis hat eine zentrale Bedeutung für die Frage, an welcher Stelle ein effektiver Geheimnisschutz ansetzen muss.

Neue rechtliche Vorgaben

Der Schutz von Know-how ist in Deutschland durch das Geschäftsgeheimnisgesetz (GeschGehG), das im April 2019 in Kraft getreten ist, erstmals umfassend systematisch und einheitlich geregelt worden. Das Gesetz dient in erster Linie der Umsetzung der europäischen Geheimnisschutz-RL 2016/943, die eine Angleichung des Know-how-Schutzes in den Mitgliedsländern der EU bewirken soll. Auch wenn im Verhältnis zum früheren Schutz, der über die §§ 17-19 des Gesetzes gegen den unlauteren Wettbewerb (UWG) vermittelt wurde, nur wenige Änderungen zu verzeichnen sind, müssen alle Geheimnisinhaber eine zentrale Neuerung beachten:

Nach der früheren Rechtsprechung war eine unternehmensbezogene Information als Geheimnis geschützt, solange die Information tatsäch-

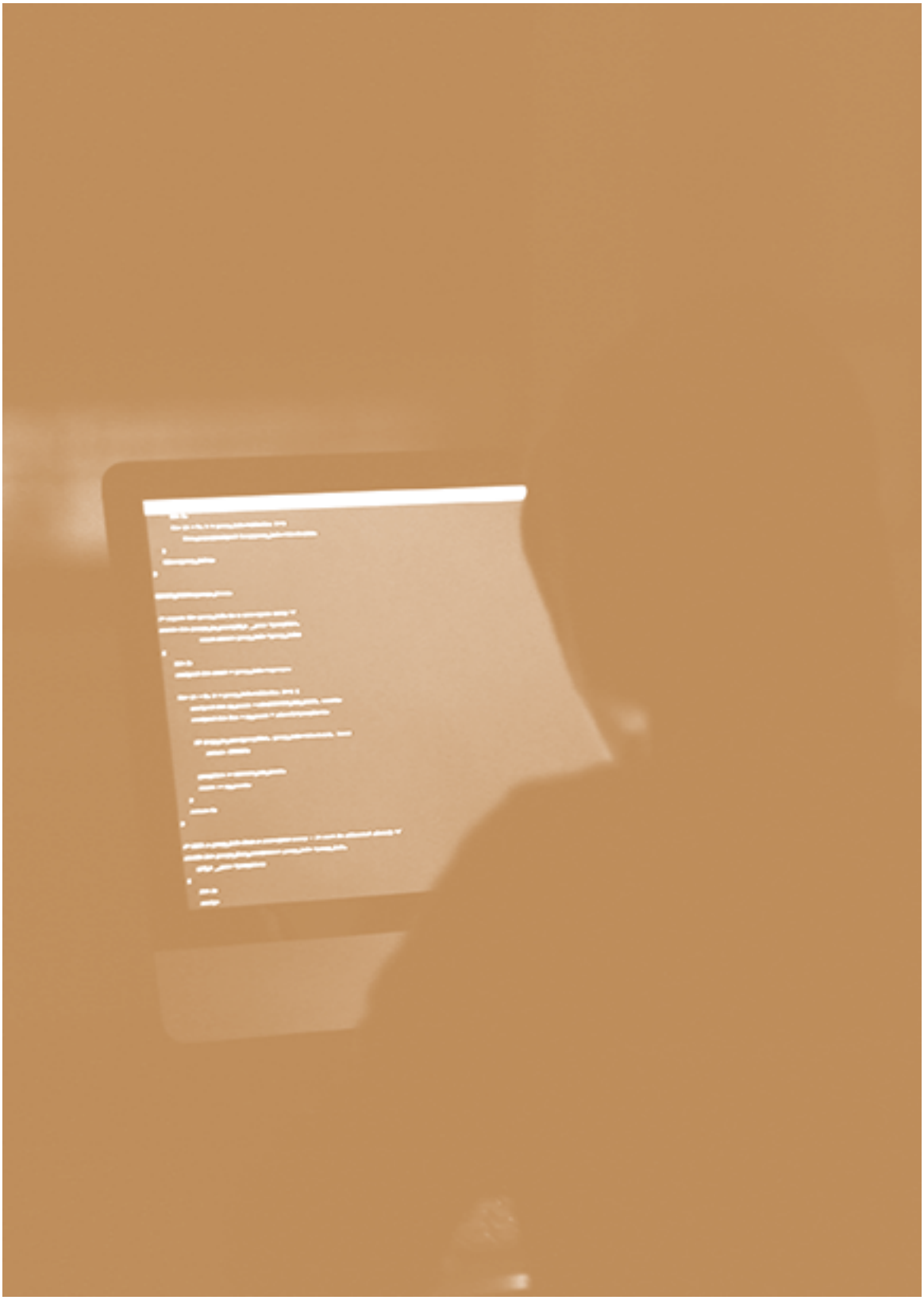
lich geheim war und ein Geheimhaltungswille bestand. Der für den Schutz erforderliche Geheimhaltungswille wurde allerdings vermutet und bildete somit keine nachzuweisende Voraussetzung für den Schutz. Nach der jetzt eingeführten Legaldefinition des Geschäftsgeheimnisses genügt dies nicht mehr. Vielmehr bildet eine Information nur dann ein rechtlich geschütztes Geschäftsgeheimnis, wenn sie Gegenstand von „angemessenen Geheimhaltungsmaßnahmen" ist (§ 2 Nr. 1 b) GeschGehG). Auch wenn das Gesetz keine konkreten Vorgaben zu bestimmten Geheimhaltungsmaßnahmen enthält, muss der Geheimnisinhaber im Fall einer Auseinandersetzung darlegen und beweisen, dass er zumindest gewisse Vorkehrungen zum Schutz seiner Geheimnisse getroffen hat. Kann der Geheimnisinhaber keine angemessenen Geheimhaltungsmaßnahmen nachweisen, so ist die entsprechende Information nicht geschützt.

Geheimhaltungsmaßnahmen

Welche Maßnahmen „angemessen" im Sinne des Gesetzes sind, wird erst im Laufe der nächsten Jahre durch die Gerichte präzisiert werden und hängt jeweils von den Umständen des Einzelfalls ab. Es ist sicherlich auch in Zukunft nicht erforderlich, alle Unternehmensdaten mit hohem finanziellen und technischen Aufwand auf Geheimdienstniveau zu schützen – ein übertriebener Aufwand wäre eben nicht „angemessen" und darf daher auch keine Voraussetzung für den Schutz bilden. Gerade bei wirtschaftlich wertvollen Geschäftsgeheimnissen muss jeder Geheimnisinhaber jedoch sorgfältig überprüfen, ob der vorhandene Schutz ausreicht oder zusätzliche Maßnahmen getroffen werden müssen. Ein Unternehmen wird im Fall einer Auseinandersetzung nur schwer argumentieren können, dass eine bestimmte Information von existenzieller Bedeutung sei, ohne Geheimhaltungsmaßnahmen darzulegen, die diese Bedeutung widerspiegeln.

Zu den naheliegenden Schutzmaßnahmen gehört zunächst eine Klassifizierung der Geheimnisse und der Abschluss von Geheimhaltungsvereinbarungen (Non Disclosure Agreements, NDA) im Verhältnis zu Geschäftspartnern und Zulieferern, wobei zweifelhaft ist, ob übliche Standardformulierungen ausreichen. Zumindest bei wichtigen Geschäftsgeheimnissen dürfte es erforderlich sein, die Geheimhaltungsvereinbarung sorgfältig auf den konkreten Einzelfall und die Nutzung des Geheimnisses durch den Vertragspartner anzupassen. Zumindest in Ausnahmefällen kann es auch geboten sein, in die Vereinbarung eine Vertragsstrafenklausel aufzunehmen, um eine Sanktionierung zu ermöglichen und vor allem die Bedeutung der Geheimhaltungspflichten zu unterstreichen. Die unterschiedslose Verwendung von Standardklauseln für alle Arten von Geheimnissen unabhängig von ihrer wirtschaftlichen Bedeutung könnte jedenfalls ein Indiz dafür sein, dass der Geheimnisinhaber für die wirklich wichtigen Informationen kein angemessenes Schutzniveau einhält.

Darüber hinaus muss der Schutz von Geschäftsgeheimnissen vor allem (auch) auf allen Ebenen der IT-Infrastruktur sichergestellt werden. Dies war schon vor Inkrafttreten des neuen Gesetzes im eigenen Interesse eines jeden Geheimnisinhabers geboten. Die geänderte Rechtslage



verschärft jedoch die Konsequenzen bei unzureichendem Schutz, indem die Durchsetzung von Ansprüchen schlicht unmöglich wird. Welche Schutzmaßnahmen geeignet und erforderlich sind, hängt auch an dieser Stelle von der Größe des Unternehmens und der Bedeutung der Information ab. Regelmäßig dürften technisch-organisatorische Maßnahmen wie die Einrichtung ordnungsgemäßer Firewalls und die Verwendung aktueller Antivirensoftware auf sämtlichen Computern zu den Mindestanforderungen gehören. Ferner ist auch an die physische Absicherung von Datenleitungen und Serverräumen zu denken.

Als zentrale Maßnahme ist in der IT auf eine strikte Durchsetzung des „Need to know"-Prinzips zu achten: Die Zugriffsberechtigungen der Mitarbeiter sollten so konfiguriert sein, dass jeder Mitarbeiter nur auf die Daten zugreifen kann, die er tatsächlich konkret für die Erfüllung seiner dienstlichen Aufgaben benötigt. Ein umfassender Zugriff auf Unternehmensinformationen ist regelmäßig auch bei Führungspersonal nicht erforderlich – auch der Leiter des Rechnungswesens benötigt keinen Zugriff auf die Forschungsdaten und der „Head of R&D" muss die Bilanzplanung für das Folgejahr nicht kennen.

Im Rahmen einer „Geheimnisschutz-Policy" sollte das Bewusstsein aller Mitarbeiter für die Notwendigkeit von Schutzmaßnahmen geschärft werden. Insbesondere sollten Regelungen für den Umgang mit Geschäftsgeheimnissen in der täglichen Arbeit, insbesondere bei der Verwendung von digitalen Kopien, getroffen werden. Der private Gebrauch der betrieblichen IT-Infrastruktur (einschließlich des E-Mail-Accounts) ist ausnahmslos zu untersagen, weil andernfalls im Fall eines Verdachts eine Untersuchung nicht oder nur sehr eingeschränkt möglich ist. Selbstverständlich ist die Verwendung privater Speichermedien und privater Computer durch Mitarbeiter ebenfalls zu verbieten. Empfehlenswert sind auch Kontroll- und Überwachungsmechanismen, welche z. B. eine auffällig hohe Zahl von Zugriffen bestimmter Personen auf bestimmte Dateien (Konstruktionspläne, Forschungsergebnisse) registrieren. Zu beachten ist, dass bei der Implementierung entsprechender Mechanismen die Zustimmung des Betriebsrats erforderlich ist, weil es sich um Überwachungsmaßnahmen nach § 87 Abs. 1 Nr. 6 BetrVG handelt. Die Verhandlung entsprechender Regelungen mit dem Betriebsrat ist mitunter mühsam, aus rechtlicher Sicht aber schon deswegen unumgänglich, weil die Ergebnisse andernfalls nicht verwertbar sind und die Überwachungsmaßnahme als solche gegebenenfalls rechtswidrig ist.

Fazit

Die Digitalisierung und die geänderte Rechtslage stellen den Know-how-Schutz vor wachsende Herausforderungen. Die nunmehr erforderlichen „angemessenen Geheimhaltungsmaßnahmen" zwingen den Geheimnisinhaber nicht dazu, mit hohen Kosten den optimalen Schutz seiner Geheimnisse sicherzustellen. Dringend geboten ist jedoch eine systematische Überprüfung und Anpassung der vorhandenen Schutzmaßnahmen und deren Dokumentation, weil andernfalls insbesondere die kurzfristige Durchsetzung von Ansprüchen kaum möglich ist.

Für sämtliche Fragen zum Know-how-Schutz stehen Ihnen gerne zur Verfügung:

Dr. Stefan Maaßen, LL.M.
0221 650 65-231
stefan.maassen@loschelder.de

Dr. Martin Brock
0221 650 65-233
martin.brock@loschelder.de

Dr. Patrick Pommerening
0221 650 65-134
patrick.pommerening@loschelder.de

In eigener Sache

Digitalisierung

Kaum ein anderes Thema offenbart derart viele Chancen und Herausforderungen für die Wirtschaft wie die digitale Transformation.
Wir begleiten Ihr Unternehmen mit unserer umfangreichen Erfahrung mit Digitalisierungsprozessen in unterschiedlichsten Branchen und Unternehmen jeglicher Größenordnung.
Ihre Ansprechpartner zu den unterschiedlichen Themen finden Sie direkt auf unserer Homepage in der neuen Rubrik „Digitalisierung“:
https://loschelder.de/de/rechtsanwaelte/rechtsberatung/digitalisierung.html

In unserer neuen Veranstaltungsreihe „Forum Digitalisierung“ machen wir Sie abseits konkreter Mandatsthemen in allen praxisrelevanten Rechtsfragen rund um die Digitalisierung fit.

Team Digitalisierung:

Dr. Detlef Grimm
Dr. Thilo Klingbeil
Dr. Stefan Maaßen
Dr. Kristina Schreiber
Dr. Felix Ebbinghaus
Dr. Hans-Georg Schreier
Dr. Simon Kohm
Dr. Stefan Freh
Dr. Patrick Pommerening
Dr. Jonas Singraven

Über „rechtAktuell“
Die Publikation „rechtAktuell“ ist eine unregelmäßig erscheinende Veröffentlichung von Loschelder und beinhaltet keinen konkreten Rechtsrat zu einem speziellen Sachverhalt. Die veröffentlichten Artikel sind allgemeine Zusammenfassungen zu aktuellen rechtlichen Fragen, gesetzgeberischen Entwicklungen und Veränderungen aufgrund neuer Entscheidungen. Wir empfehlen deshalb dringend, bei konkreten Fragen einen Rechtsanwalt unserer Sozietät zu konsultieren. Dieser wird Ihre speziellen Fragen unter Berücksichtigung des Sachverhaltes und Ihrer Bedürfnisse gerne beantworten. Diese Veröffentlichung kann auf unserer Homepage unter www.loschelder.de abgerufen werden. Dort finden Sie auch weitere Veröffentlichungen unserer Sozietät.

Bezugswege
Normalerweise erhalten Sie „rechtAktuell“ im gewohnten Papierformat. Möchten Sie zukünftig „rechtAktuell“ gerne im PDF-Format beziehen? Dann schicken Sie uns bitte eine kurze Nachricht an: recht.aktuell@loschelder.de

Datenschutzhinweise
Unter www.loschelder.de/de/datenschutz; auf Anfrage per Post und E-Mail.

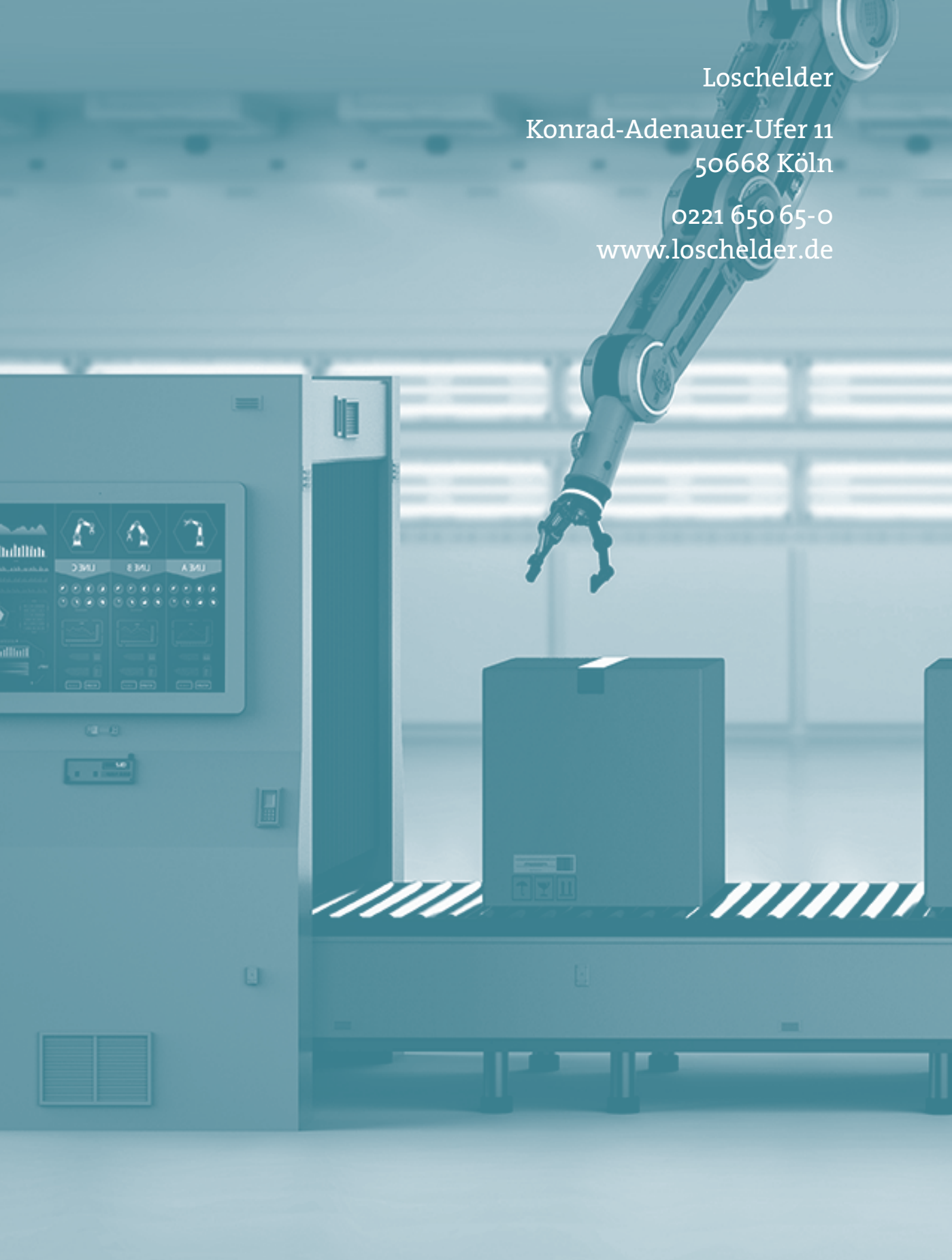
Impressum

Herausgeber:
LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB

Konrad-Adenauer-Ufer 11
50668 Köln
Tel. 0221 65065-0
Fax 0221 65065-110
info@loschelder.de
www.loschelder.de

Konzept, Gestaltung:
wiehl, Co.

Fotografie:
iStock/gettyimages, Asbach



Loschelder

Konrad-Adenauer-Ufer 11
50668 Köln

0221 650 65-0
www.loschelder.de