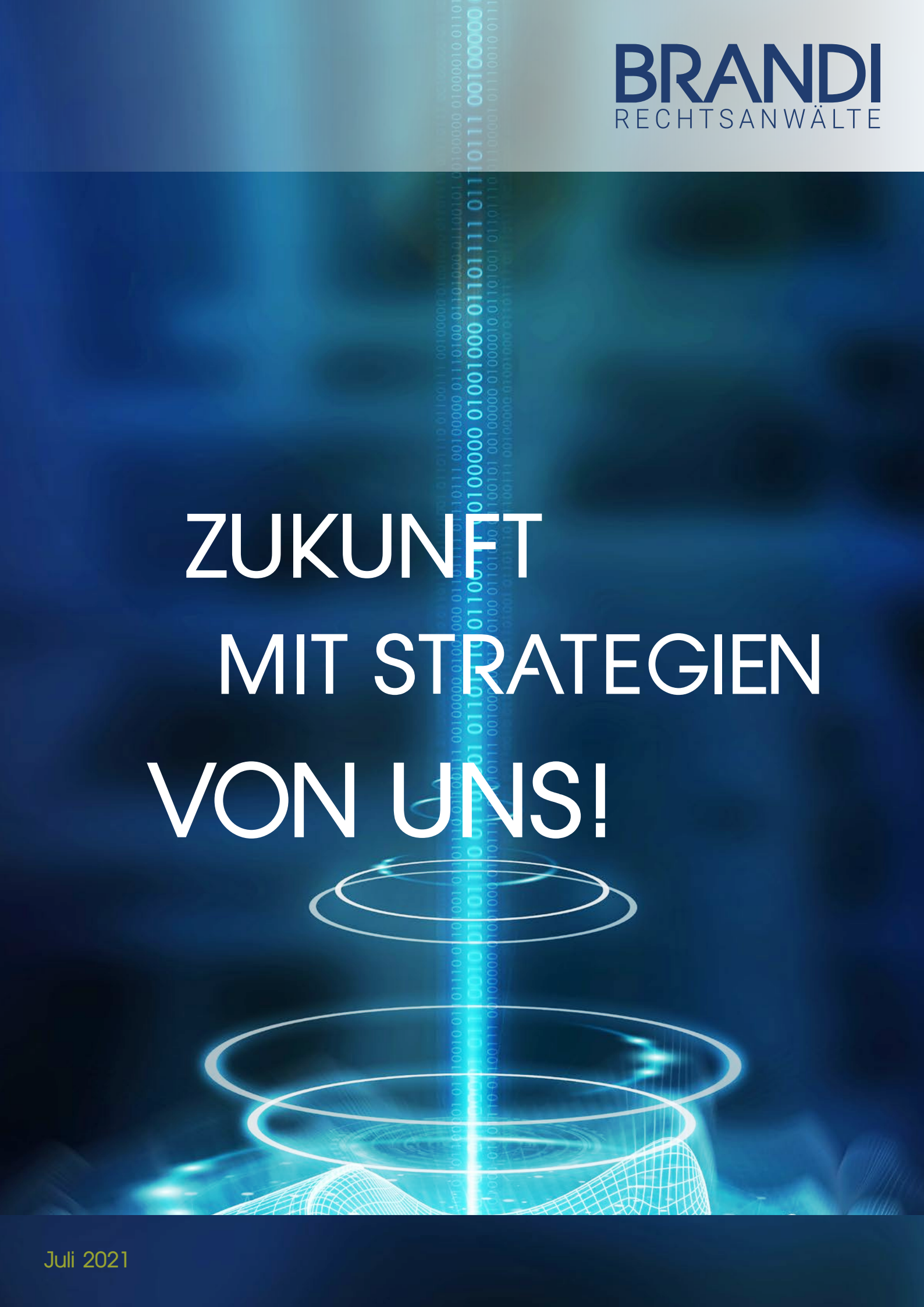
BRANDI
RECHTSANWÄLTE

ZUKUNFT MIT STRATEGIEN VON UNS!



Juli 2021

Liebe Leserinnen und liebe Leser,

wir freuen uns sehr, Ihnen mit der Juli-Ausgabe unseres BRANDI Reports wieder Interessantes zum Lesen bieten zu können.

Das sogenannte „Lieferkettengesetz“ ist beschlossen. Was Sie berücksichtigen sollten, lesen Sie in dieser Ausgabe. Ob ein Insolvenzverwalter Zahlungen zur Insolvenzmasse zurückholen kann, was die wesentlichen Regelungsaspekte der Incoterms® 2020 sind und Weiteres erläutern Mitglieder unserer Kompetenzgruppe Handel & Vertrieb.

In unserem Live Event „Update Vertriebsrecht“ am 10. Juni 2021 wurden diese Themen neben anderen behandelt.

Unsere Kompetenzgruppe IT & Datenschutz hat die Diskussion der Onlineveranstaltung zum Datenschutzrechtstag vom 07. Mai 2021 informativ für Sie zusammengefasst.

Außerdem berichtet das Team IT & Datenschutz neben anderen Beiträgen darüber, was die gesteigerten Verbraucherschutzanforderungen an Konsequenzen für Unternehmer mit sich bringen, den Zusammenhang von Datenschutzrecht und Schmerzensgeld oder wie sich Account-Nutzung über Instagram-Insights gegenüber personenbezogenen Daten verhält.

Bekanntheit und hohe Qualitätsvorstellungen anderer Produkte für einen Imagetransfer zu nutzen, kann rechtliche Konsequenzen haben. Auch der Klick auf ein Foto kann für einen Herausgeber teuer werden. Diese und weitere Beiträge haben wir unter „Verschiedenes“ für Sie zusammengestellt.

Wir wünschen Ihnen eine schöne Sommerzeit.
Ihr BRANDI Team

AKTUELLES

DATENSCHUTZRECHTSTAG – 07. MAI 2021

Anlässlich des dreijährigen Jubiläums der Datenschutz-Grundverordnung (DSGVO) hat die BRANDI-Kompetenzgruppe für IT & Datenschutz am 07. Mai 2021 erfolgreich einen Datenschutzrechtstag veranstaltet. Mitschnitte aus der Veranstaltung finden Sie auf unserer Homepage unter „Veranstaltungen“ oder als Podcast unter „News/Podcast“.

UPDATE VERTRIEBSRECHT – 10. JUNI 2021

Nähere Informationen zum Update Vertriebsrecht, veranstaltet von unserer Kompetenzgruppe Handel & Vertrieb, sind ebenfalls auf unserer Homepage unter „Veranstaltungen“, sowie in diesem BRANDI Report zu finden.

BRANDI BLOG

Neu auf unserer Homepage: BRANDI bloggt zu aktuellen und interessanten Themen.

FRAGEN AN CHRISTIAN RÖDDING

WARUM BRANDI?

Der Kontakt zu BRANDI bestand schon länger: Während des Studiums habe ich ein Praktikum bei BRANDI absolviert; im Referendariat kam dann die Anwaltsstation hinzu. Beide Male konnte ich mich davon überzeugen, wie kollegial der Umgang miteinander bei BRANDI abläuft – es ist gerade kein Büro, in dem jeder für sich seine Zeit „absitzt". Das überträgt sich auch auf die Mandate: Hier gibt es keine anonymen Bearbeiter, stattdessen ist jeder von Anfang an auch nach außen hin tätig.

WAS TREIBT MICH AN?

Als Anwalt kann ich unsere Mandanten frühzeitig begleiten. Ich fange also nicht erst dann an, wenn es schon „zu spät" ist, sondern kann gemeinsam mit den Mandanten Ideen entwickeln und gestalten, damit es zu Rechtsstreitigkeiten gar nicht erst kommt. Es ist jedes Mal eine neue und spannende Herausforderung, Lösungen zu finden, die sowohl rechtlich wasserdicht als auch wirtschaftlich vernünftig sind.

Christian Rödding
Rechtsanwalt
christian.roedding@brandi.net

AUSSER DEM JOB GIBT ES NOCH...?

Den (übrigens auch nichtjuristischen!) Freundeskreis, viel Musik (mit der Geige in kleiner Runde oder in der Orchestergesellschaft Detmold), ehrenamtliche Arbeit in der Kommunalpolitik und kürzere oder längere Ausflüge in die Natur.

HIGHLIGHTS AUS MEINER HEIMAT?

Als „Rückkehrer" in die Detmolder Heimat habe ich mich besonders auf die kulturelle Vielfalt in der Stadt gefreut – das musste pandemiebedingt natürlich noch etwas warten. Aber auch die Natur direkt vor der Haustür mit unzähligen Wanderwegen hat es mir sehr einfach gemacht, mich nach meinem Studium in Halle (Saale) wieder für meine alte Heimat zu entscheiden.

Dr. Sörren Kiene

„Lieferkettengesetz“ – erhöhte Sorgfaltsanforderungen und -pflichten in der Lieferkette

Am 11. Juni 2021 hat der Bundestag das Lieferkettensorgfaltspflichtengesetz (Gesetz über die unternehmerischen Sorgfaltspflichten zur Vermeidung von Menschenrechtsverletzungen in Lieferketten) verabschiedet, das am 1. Januar 2023 in Kraft treten wird. In der medialen Berichterstattung wird es häufig nur als „Lieferkettengesetz“ bezeichnet. Insbesondere beim Abschluss langjähriger Rahmenlieferverträge sollten Unternehmen daher jetzt schon überlegen, Vorkehrungen zu treffen, um die späteren Vorgaben einhalten zu können. Denn die neue Gesetzeslage bedeutet für Unternehmen Handlungs- und Aktualisierungsbedarf, insbesondere in den Bereichen Compliance und Vertragsgestaltung.

Das Lieferkettengesetz hat sich eine Verbesserung der weltweiten Menschenrechtslage entlang der gesamten Lieferkette zum Ziel gesetzt. Die Lieferkette im Sinne des Gesetzes erstreckt sich auf den gesamten Produktherstellungsprozess, angefangen von der Gewinnung von notwendigen Rohstoffen bis hin zur Lieferung des Produkts an den Endkunden. Regelungsgegenstand sind ferner auch Umweltbelange, beispielweise im Rahmen des Abfallhandels, soweit sie Risiken für Menschenrechte begründen können. Mithilfe des Gesetzes sollen gerechte Arbeitsbedingungen geschaffen werden, Menschen sollen von Zwangsarbeit und Kinder von Kinderarbeit befreit werden. Um dies zu erreichen, nimmt das Lieferkettengesetz Unternehmen in die Pflicht. Dabei differenziert dieses Gesetz zwischen den Sorgfaltspflichten im Verhältnis zu unmittelbaren Zulieferern einerseits und im Verhältnis zu mittelbaren Zulieferern andererseits. Doch was genau müssen Unternehmen künftig im Rahmen ihres eigenen Geschäftsbereichs, aber auch im Verhältnis zu Zulieferern beachten, um die Sorgfaltspflichten zu erfüllen?

Zunächst lässt sich festhalten, dass das Lieferkettengesetz ab dem 1. Januar 2023 für Unternehmen gilt, die ihren Sitz im Inland haben und dort mindestens 3.000 Arbeitnehmer (einschließlich ins Ausland entsandter Arbeitnehmer) beschäftigen. Dieser Schwellwert gilt auch für ausländische Unternehmen mit Zweigniederlassung in Deutschland. Ab dem 1. Januar 2024 beträgt der genannte Schwellwert 1.000 Arbeitnehmer, sodass das Lieferkettengesetz dann noch deutlich mehr Unternehmen betreffen wird.

Die betroffenen Unternehmen müssen sich bemühen, dass es weder im eigenen Geschäftsbereich noch in der Lieferkette zu Menschenrechtsverletzungen kommt. Dabei sind insbesondere folgende Maßnahmen umzusetzen:

> Risikomanagement: Unternehmen müssen unter anderem ein angemessenes Risikomanagement einführen und wirksam umsetzen, wodurch potentiell negative Auswirkungen auf die Menschenrechte abgewendet werden.
>
> Risikoanalyse: Unternehmen wird von Gesetzes wegen auferlegt, zu analysieren, ob ein Risiko dahingehend besteht, dass ihre eigenen geschäftlichen Handlungen oder geschäftliche Handlungen in der Lieferkette Menschenrechte verletzen.
>
> Grundsatzerklärung: Unternehmen sind verpflichtet, eine sogenannte Grundsatzerklärung zu ihrer Menschenrechtsstrategie zu verabschieden. Diese Grundsatzerklärung muss unter anderem eine Beschreibung des Verfahrens enthalten, wie das Unternehmen seinen Sorgfaltsanforderungen nachkommt. Außerdem muss sie die menschenrechts- und umweltbezogenen Erwartungen, die das Unternehmen an seine Beschäftigten und Zulieferer hat, enthalten.
>
> Präventions- und Abhilfemaßnahmen: Die betroffenen Unternehmen sind verpflichtet, ihre Lieferanten sorgfältig auszuwählen und zu kontrollieren, Schulungen durchzuführen und Verträge nachhaltig zu gestalten.
>
> Beschwerdemechanismus: Zudem müssen Unternehmen einen Beschwerdemechanismus einrichten, über den Betroffene und Personen, die Kenntnis von möglichen Verletzungen haben, auf menschenrechtliche Risiken und Verletzungen hinweisen können.
>
> Berichterstattung: Schließlich müssen die Unternehmen transparent öffentlich Bericht über die Erfüllung der menschenrechtsbezogenen Sorgfaltspflichten erstatten. Es ist ein jährlicher Bericht zu erstellen, der bei der zuständigen Behörde einzureichen ist.

Kann ein Unternehmen eine Verletzung beim unmittelbaren Zulieferer nicht in absehbarer Zeit beenden, muss es einen konkreten Plan zur Minimierung und Vermeidung erstellen.

In Bezug auf den mittelbaren Zulieferer gelten die Sorgfaltspflichten nur anlassbezogen und nicht generell: Erlangt das Unternehmen Kenntnis von einem möglichen Verstoß beim mittelbaren Zulieferer, so hat es unverzüglich eine Risikoanalyse durchzuführen, ein Konzept zur Minimierung und Vermeidung umzusetzen und angemessene Präventionsmaßnahmen gegenüber dem Verursacher zu verankern.

Es stellt sich weiter die Frage, unter welchen Voraussetzungen Geschäftsbeziehungen beendet werden müssen: Ein Abbruch der Geschäftsbeziehungen ist nur dann geboten, wenn eine schwerwiegende Menschenrechtsverletzung festgestellt wurde und die bisherigen Maßnahmen des Konzepts innerhalb einer gesetzten Frist nicht erfolgreich sind. Ziel des Gesetzes ist es nämlich nicht Geschäftsbeziehungen zu beenden, sondern den Menschenrechtsschutz zu stärken.

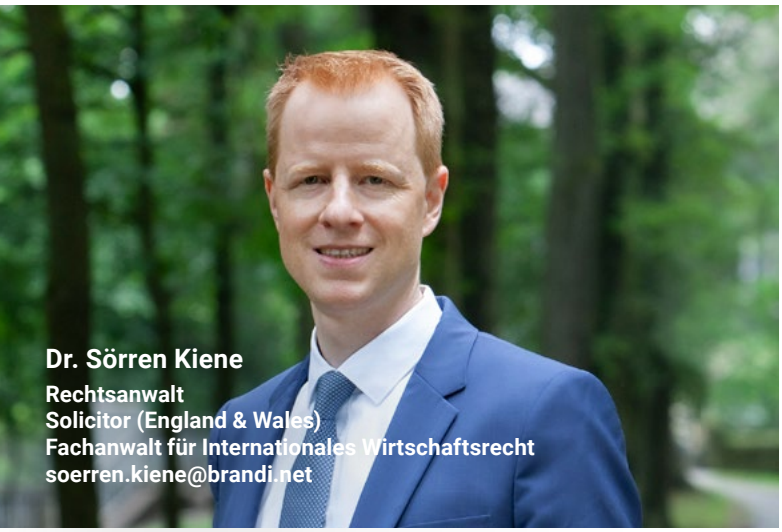
Damit dieses Ziel auch erreicht und geschützt wird, sanktioniert das Gesetz etwaige Verstöße mit Bußgeldern. Bei Verstößen gegen Sorgfaltspflichten und Berichtspflichten droht ein Bußgeld von bis zu 800.000 Euro. Bei Verstößen gegen die Pflicht zur Einleitung von Abhilfemaßnahmen bei einem unmittelbaren Zulieferer droht Unternehmen mit einem durchschnittlichen Jahresumsatz von mehr als 400 Millionen Euro eine Geldbuße von bis zu 2 % des durchschnittlichen Jahresumsatzes. Zudem ist es möglich, dass Unternehmen, die sich nicht gesetzeskonform verhalten, von öffentlichen Ausschreibungen für eine begrenzte Zeit ausgeschlossen werden.

Die vorstehenden Ausführungen zeigen, dass das Lieferkettengesetz den Unternehmen erhöhte Sorgfaltspflichten auferlegt

und Verstöße nicht sanktionslos lassen wird. Demgegenüber sieht das Lieferkettengesetz zivilrechtliche Haftungserweiterungen nicht vor; es gilt weiterhin die zivilrechtliche Haftung nach deutschem und gegebenenfalls ausländischem Recht.

Ausblick und Fazit:
Betroffene Unternehmen sind gut beraten, die Zeit bis zum Inkrafttreten zu nutzen. Selbst wenn Unternehmen nicht direkt Adressaten des Lieferkettengesetzes sind, ist zu erwarten, dass sie davon mittelbar betroffen sein werden. Denn bei Lieferungen an betroffene Kunden, die die Arbeitnehmerschwellen überschreiten, ist davon auszugehen, dass diese Kunden zukünftig entsprechende vertragliche Regelungen zur Einhaltung des Lieferkettengesetzes verlangen werden. Jedenfalls mittelbar dürfte damit eine Vielzahl von Unternehmen, auch unterhalb der maßgeblichen Mitarbeiterzahlen, mit dem Lieferkettengesetz in Berührung kommen. Unabhängig von den deutschen Regelungen zeichnet sich am Horizont schon weitgehender Handlungsbedarf ab: Auch die Europäische Union hat mit Arbeiten und ersten Überlegungen an einem europaweit gültigen Lieferkettengesetz begonnen. Die Informationslage ist dazu noch wenig belastbar, aber es scheint noch strengere Regeln zu statuieren. Das Europaparlament fordert derzeit zum einen, dass bereits Unternehmen mit 250 Mitarbeitern in das Gesetz mit einbezogen werden sollen. Zum anderen sollen die erhöhten Sorgfaltspflichten, die gegenüber den unmittelbaren Zulieferern bestehen, auch gegenüber den mittelbaren Zulieferern gelten. Eine Verschärfung des derzeitigen Gesetzesentwurfs durch eine einheitliche europäische Regelung ist somit nicht ausgeschlossen.

Auch deshalb heißt es, die mit dem Lieferkettengesetz zusammenhängenden Fragestellungen nicht auf die lange Bank zu schieben. Denn eines dürfte jetzt schon feststehen: Unternehmen müssen aufrüsten, sowohl in organisatorischer als auch in vertragsgestalterischer Hinsicht, um den Anforderungen des Lieferkettengesetzes gerecht werden zu können.



Dr. Sörren Kiene
Rechtsanwalt
Solicitor (England & Wales)
Fachanwalt für Internationales Wirtschaftsrecht
soerren.kiene@brandi.net

Dr. Birgit Jaenicke

Force Majeure – Sinn und Unsinn von Force Majeure-Klauseln

Force Majeure-Klauseln sind seit Beginn der Covid-19 Pandemie eine der am häufigsten nachgefragten Einzelklauseln in Vertriebsverträgen geworden. Force Majeure oder deren deutsches Pendant, die „höhere Gewalt", vom BGH als „betriebsfremdes, von außen herbeigeführtes Ereignis, das nach menschlicher Einsicht und Erfahrung unvorhersehbar ist" beschrieben, ist in den letzten Monaten vom juristischen Gedankenspiel zur allgemeinen Erfahrung geworden.

Bislang schienen Force Majeure-Klauseln in deutsch-deutschen Vertriebsverträgen verzichtbar und in grenzüberschreitenden Verträgen von geringer Relevanz. In der Praxis des letzten Jahres hat sich aber gezeigt, dass die vom deutschen Gesetzgeber zur Verfügung gestellten Lösungen über die objektive oder subjektive „Unmöglichkeit" oder die „Störung der Geschäftsgrundlage" ebenso wie die Befreiung von Schadenersatzverpflichtungen des UN-Kaufrechts weit davon entfernt sind, den Vertragsparteien eine schnelle und rechtssichere Lösung in schwierigen Situationen zu bieten.

Tatsächlich kann eine Force Majeure-Klausel hilfreich sein – wenn sie gut gemacht und auf die Interessen der Parteien abgestimmt ist. Dazu gehört nicht nur eine sinnvolle Definition der Umstände, unter denen Force Majeure eintritt. Vor allem bei den aus einer Force Majeure Situation abgeleiteten Rechtsfolgen wird oft zu kurz gedacht: So ist dem Lieferanten einer Sondermaschine möglicherweise gar nicht damit gedient, wenn die bei ihm eingetretene Force Majeure Situation seinem Vertragspartner zu einer erleichterten Vertragsaufhebung verhilft.

Was eine Force Majeure-Klausel leisten kann und wie sie aussehen sollte, war Gegenstand des „Update Vertriebsrecht".

Dr. Birgit Jaenicke
Rechtsanwältin und Mediatorin (DAA)
Fachanwältin für Internationales Wirtschaftsrecht
birgit.jaenicke@brandi.net

Dr. Sörren Kiene

Die Incoterms® 2020

Die Internationale Handelskammer in Paris (ICC) hat anlässlich Ihres 100jährigen Bestehens die neuen Incoterms® 2020 herausgegeben. Die Incoterms (International Commercial Terms) werden auch als internationale Handelsklausel bezeichnet. Wichtig für den Anwender ist, dass die Incoterms® 2020 entgegen ihrer Bezeichnung auch im reinen Inlandsgeschäft eingesetzt werden können und nach Möglichkeit auch sollten.

Da die ICC kein Gesetzgeber ist, sind die vorherigen Fassungen der Incoterms® mit der Veröffentlichung der Incoterms® 2020 nicht etwa abgeschafft. Wer möchte, kann selbstverständlich auch noch die Incoterms® 2010 oder ältere Fassungen verwenden. Entscheidend ist, dass sich die Parteien auf eine Fassung

einigen. Geben die Parteien keine Fassung an, ergibt die Auslegung in aller Regel, dass bei ab dem 01.01.2020 abgeschlossenen Verträgen die Incoterms® 2020 gelten sollen.

Da die Parteien also auch weiterhin die Incoterms® 2010 verwenden können, besteht mit anderen Worten auch keine Pflicht, jetzt alle internen Prozesse sofort auf die Incoterms® 2020 umzustellen. Zunächst sollte der Anwender die Änderungen sowie daraus etwaig resultierende Anpassungen im eigenen Unternehmen prüfen.

Die Incoterms® 2020 sind nur anwendbar auf Kaufverträge und Werklieferungsverträge. Sie sind in der Praxis ein außerordentlich gutes Mittel, um wichtige rechtliche Fragen, wie insbesondere den Kosten- und Gefahrenübergang vom Verkäufer auf den Käufer, die Pflichtenaufteilung zur Ausfuhr-, Durchfuhr- und Einfuhrfreimachung sowie etwaige Versicherungspflichten verbindlich und rechtssicher zu vereinbaren. Streng verknüpft mit der Frage des Gefahrenübergangs ist auch der Begriff der „Lieferung". Hinter diesem, auch im täglichen Sprachgebrauch verwendeten, Begriff steht ein gesamtes rechtliches Konzept, das zwar im Ergebnis nicht sonderlich kompliziert ist, aber erfahrungsgemäß nicht durchgehend vollständig durchdrungen wird. Insbesondere im angloamerikanischen Rechtskreis werden Begriffe wie „delivery" und „shipment" häufig synonym verwendet, obwohl „delivery" und shipment" keinesfalls zusammenfallen müssen. „Delivery" bedeutet letztlich „Lieferung", bezeichnet also den Ort, in dem die Gefahr (d. h. das Risiko) des zufälligen Untergangs der Ware vom Verkäufer auf den Käufer übergeht. Mit anderen Worten erhält der Verkäufer dennoch seinen Kaufpreis und muss die Ware nicht etwa noch einmal liefern, wenn sie nach dem Gefahrenübergang aufgrund eines zufälligen Ereignisses untergeht. Der Begriff „shipment" ist dagegen kein rechtlicher Begriff, sondern bezeichnet nur die rein tatsächliche Versendung. Diese kann aber vor oder nach der Lieferung liegen. So geht beispielsweise die Gefahr bei einer vereinbarten Lieferung „EXW [Ort] Incoterms® 2020" schon mit der Bereitstellung der Ware an den Käufer über. Die Versendung erfolgt erst danach.

Die wesentlichen Regelungsaspekte der Incoterms® 2020 sind folgende:

> Lieferung
>
> Kostenübergang vom Verkäufer auf den Käufer
>
> Gefahrübergang vom Verkäufer auf den Käufer
>
> Etwaige Versicherungspflichten
>
> Zuordnung der Pflichten zur Ausfuhr-, Durchfuhr- und Einfuhrfreimachung

Damit zeigt sich aber auch, was die Incoterms® 2020 nicht leisten können. Dazu gehören insbesondere Fragestellungen wie a) ob überhaupt ein Kaufvertrag abgeschlossen wurde, b) welche Beschaffenheiten oder Spezifikationen die Ware aufweisen soll, c) Zeit, Ort, Zahlungsweise oder Währung der Bezahlung sowie d) Rechtsfolgen bei Pflichtverletzungen aus einem Kaufvertrag, z. B. bei Lieferung mangelhafter Ware. Der Rechtsanwender sollte sich daher von dem Begriff „Lieferbedingung", wie die einzelnen Incoterms-Klauseln auch häufig bezeichnet werden, nicht irritieren lassen. Die Incoterms-Klauseln regeln zwar die Lieferbedingung dergestalt, dass sie klar festlegen, wann die Gefahr vom Verkäufer auf den Käufer übergeht, sie sind aber nicht gleichzusetzen mit etwaigen „Lieferbedingungen" in Form von Zahlungs- und Lieferbedingungen oder sonstigen Allgemeinen Geschäftsbedingungen. Damit regeln die Incoterms® 2020 auch nicht Aspekte wie den Eigentumsübergang oder – bei grenzüberschreitenden Sachverhalten besonders wichtig – die Frage des anwendbaren Rechts oder beinhalten eine Gerichtsstandsvereinbarung.

Gemäß dem bewährten Aufbau regeln auch die Incoterms® 2020 in ihren Regeln A1 bis A10 die Pflichten des Verkäufers und in den Regeln B1 bis B10 die Pflichten des Käufers. Die sogenannten „erläuternden Kommentare" zu Beginn jeder Incoterm-Klausel stellen eine hilfreiche und lesenswerte Einführung in die jeweilige Incoterm-Klausel dar. Jedem Rechtsanwender sei empfohlen, sich diese erläuternden Kommentare zu der von ihm beabsichtigten Incoterm-Klausel durchzulesen, bevor er die jeweilige Incoterm-Klausel anwendet.

Die ICC hat im Zuge der Neufassung der Incoterms® 2020 eine Vielzahl von Änderungen vorgenommen, die insgesamt die Incoterms® 2020 noch benutzerfreundlicher gestalten. Besonders ins Auge sticht hier wohl der Wegfall der Klausel DAT (delivered at terminal) Incoterms® 2010 bzw. die Umgestaltung der Klausel DAT Incoterms® 2010 zur Klausel DPU (delivered at place unloaded) Incoterms® 2020. Während das Terminal bei der Klausel DAT Incoterms® 2010 durchaus an jedem beliebigen Ort sein durfte, herrschte bei vielen Rechtsanwendern offenbar die Fehlvorstellung vor, dass das Terminal stets an einem Hafen sein musste. Wohl aus diesem Grund wurde die Klausel DAT Incoterms® 2010 kaum verwendet. Die Änderung hin zur Klausel DPU Incoterms® 2020 sorgt hier für erfreuliche Klarstellung und dürfte dafür sorgen, dass die Klausel sehr viel häufiger angewendet wird.

Neben einer geänderten Reihenfolge bei den Regeln (A1 bis A10 und B1 bis B10) ist es für den Rechtsanwender von entscheidender Bedeutung, dass der abzuschließende Versicherungsschutz bei den Klauseln CIP und CIF Incoterms® 2020 nunmehr unterschiedlich ist. Während bei den Incoterms® 2010 bei den Klauseln CIF und CIP stets Versicherungsschutz nach den Klauseln (C) der Institute Cargo Clauses eingedeckt werden musste, gilt dieser Versicherungsschutz nun nur noch bei CIF Incoterms® 2020. Bei der Klausel CIP Incoterms® 2020 muss der Verkäufer dagegen sehr viel weitgehenderen Schutz eindecken, nämlich nach den Klauseln (A) der Institute Cargo Clauses. Der damit verbundene Versicherungsschutz wird häufig auch als „all risk"-Versicherung bezeichnet, da die Versicherung bei diesem Versicherungsschutz nur in sehr seltenen Ausnahmefällen von einer Einstandspflicht befreit wäre. Generell ist diese Änderung bei den Incoterms® für den Verkäufer ein guter Anlass, einmal zu prüfen, wie umfangreich denn der, typischerweise über Jahresverträge eingedeckte, Versicherungsschutz ist und ob er den erforderlichen Anforderungen gerecht wird. Aber auch Käufer sollten einmal prüfen, ob der sehr eingeschränkte Versicherungsschutz bei CIF Incoterms® 2020 tatsächlich dem eigenen Interesse gerecht wird – häufig wird dies nicht der Fall sein. Die Erfahrung zeigt, dass weder Käufer noch Verkäufer über den Ver-

sicherungsumfang wirklich informiert sind. Die Tatsache allein, dass Versicherungsschutz besteht (in welchem Umfang auch immer), scheint in der Praxis häufig beiden zu reichen, was angesichts der damit verbundenen Risiken doch erstaunt.

Für Verkäufer, die ihre Kaufpreiszahlungen häufig über Akkreditive absichern, bieten die Incoterms® 2020 bei der Klausel FCA eine zusätzliche interessante Neuerung. Nach den Incoterms® 2020 können sich Verkäufer und Käufer bei der Klausel FCA darüber einigen, dass der Käufer seinen – von ihm zu beauftragenden Frachtführer – anweist, dass dieser dem Verkäufer ein Bordkonnossement aushändigt. Dieses kann dann wiederum das notwendige Dokument sein, um eine Zahlung aus einem Akkreditiv zu erlangen. So schön sich diese Neuerung anhört, so ist dem Verkäufer dennoch zu raten, sich möglichst unabhängig vom Käufer zu machen. Der Verkäufer wird nicht rechtzeitig gerichtliche Hilfe in Anspruch nehmen können, sollte der Käufer abredewidrig keine derartige Weisung an seinen Frachtführer erteilen. Dem Verkäufer ist daher eher anzuraten, von der, bei der Klausel FCA schon durch die Incoterms® 2010 geschaffenen, Möglichkeit Gebrauch zu machen, selbst den Frachtvertrag abzuschließen, aber auf Gefahr und Kosten des Käufers.

In der Fachliteratur relativ wenig Beachtung findet die Besonderheit, dass die Incoterms nicht nur Fragen der Gefahrtragung und weitere Themenaspekte, wie oben erläutert, regeln, sondern indirekt auch entscheidenden Einfluss auf die Frage der internationalen Zuständigkeit der Gerichte haben können. Zwar ist mit den Incoterms® 2020 keine Gerichtsstandsvereinbarung verbunden, dennoch können sie Auswirkungen darauf haben, welches Gericht im Streitfalle zuständig wäre. Da es im internationalen Rechtsverkehr relativ umständlich ist, zumindest über Allgemeine Geschäftsbedingungen eine wirksame Gerichtsstandsvereinbarung abzuschließen, verwundert diese Bestandsaufnahme doch sehr. Nach den europäischen Zuständigkeitsvorschriften kann der Verkäufer einen innerhalb des Europäischen Wirtschaftsraums ansässigen Käufer am sogenannten „Erfüllungsort“ verklagen. Dieser Erfüllungsort liegt bei Kaufverträgen an dem Ort, an den die Ware geliefert wurde. Nach der Rechtsprechung des Europäischen Gerichtshofs ist zur Bestimmung des Lieferortes häufig auch auf die Incoterms® zurückzugreifen. Zwar gilt dies beispielsweise nicht, wenn die Parteien eine anderweitige Gerichtsstandsvereinbarung abgeschlossen haben. Auch sei es Aufgabe des Gerichts zu prüfen, ob mit der Wahl der Incoterms®-Klausel nur eine Kostentragung verbunden sei. Dennoch kann der Verkäufer bei sorgsamer Wahl der „richtigen“ Incoterms®-Klausel dafür sorgen, dass er im Streitfalle mit einem im Europäischen Wirtschaftsraum ansässigen Käufer seine Forderungen vor seinen Heimatgerichten einklagen kann.

Abschließend seien nachfolgend noch die wichtigsten Empfehlungen für eine richtige Anwendung der Incoterms® 2020 aufgeführt:

> Vermeiden Sie wo immer möglich Begriffe wie „frei Haus“, „frei Baustelle“ etc. Diese Begriffe sind keine Incoterms® und ihr rechtlicher Inhalt ist alles andere als klar.
>
> Verwenden Sie die Klauseln FAS, FOB, CIF, CFR Incoterms® 2020 ausschließlich bei See- und Binnenschiffstransporten.
>
> Geben Sie bei den C-Klauseln möglichst sowohl den Liefer- als auch den Bestimmungsort an.
>
> Vermeiden Sie als Verkäufer möglichst die Klausel FOB im Containerverkehr, da die Gefahr bei dieser Klausel zu einem Zeitpunkt übergeht, in dem Sie gar keinen Zugriff mehr auf die Ware haben.
>
> Vermeiden Sie im Auslandsgeschäft die „Extremklauseln“ EXW und DDP Incoterms® 2020.
>
> Geben Sie immer die von Ihnen gewünschte Fassung der Incoterms an, beispielsweise „[Ort] Incoterms 2020“.
>
> Geben Sie den Ort möglichst genau an.

Dr. Bernhard König

Wie gewonnen – so zerronnen

Insolvenzverwalter können vor Insolvenzantrag geleistete Zahlungen durch Anfechtung zurückholen.

„Da haben wir ja noch mal Glück gehabt“, denkt der Mittelständler, als er in der Zeitung liest, sein Kunde habe Insolvenzantrag gestellt.

Er hatte noch rückständige Forderungen in den Monaten vor Insolvenzeröffnung eintreiben können, allerdings erst nach massiven Drohungen mit rechtlichen Schritten oder mit einem Insolvenzantrag.

Die Annahme, keinen Schaden erlitten zu haben, stellt sich als Trugschluss heraus: Zwei Jahre nach Insolvenzeröffnung erhält er einen Brief des Insolvenzverwalters, der ihm mitteilt, die damaligen Zahlungen würden angefochten, er möge innerhalb von einem Monat die erhaltenen Beträge an die Insolvenzmasse zurückzahlen.

Anfechtungszeitraum zwischen einem Monat und 10 Jahren
Prüft der Insolvenzverwalter, ob er Rechtshandlungen vor Insolvenzeröffnungsantrag rückgängig machen und insbesondere Zahlungen zur Insolvenzmasse zurückholen kann, kann sich seine Prüfung auf Zeiträume von bis zu 10 Jahren vor Insolvenzeröffnungsantrag erstrecken.

Der Insolvenzverwalter kann mit der Anfechtung in Zeiträume vor Stellung des Insolvenzantrags „zurückgreifen“, wobei die Zeiträume und die Voraussetzungen für eine Anfechtung unterschiedlich sind:

> 10 Jahre zurück können Rechtshandlungen des Schuldners angefochten werden, wenn er mit dem Vorsatz, Gläubiger zu benachteiligen, gehandelt hat und der Gläubiger diesen Vorsatz kannte (wobei die Kenntnis vermutet wird, wenn er wusste, dass Zahlungsunfähigkeit drohte und die Handlung die Gläubiger benachteiligte).
>
> 4 Jahre zurück kann der Insolvenzverwalter anfechten, wenn der Schuldner dem Gläubiger eine Sicherung für Forderungen oder Befriedigung von Forderungen gewährt hat, mit dem Vorsatz, Gläubiger zu benachteiligen und der Gläubiger das wusste.

4 Jahre zurückgreifen kann der Insolvenzverwalter, wenn der Schuldner unentgeltliche Leistungen erbracht hat.

3 Monate zurückgreifen kann der Insolvenzverwalter bei Rechtsgeschäften des Schuldners, die die Insolvenzgläubiger unmittelbar benachteiligt haben, wenn der Schuldner schon zahlungsunfähig war und der Gläubiger das wusste oder anhand von Indizien erkennen konnte.

Bis zu 3 Monate zurückgreifen kann der Insolvenzverwalter bei Rechtshandlungen, die mit kongruenter oder inkongruenter Deckung verbunden waren, wobei die Anfechtungsgründe dann davon abhängen, ob der Schuldner in diesen Zeitpunkten schon zahlungsunfähig war und was der Gläubiger – ggf. aufgrund von Indizien – davon wusste.

Anfechten kann der Insolvenzverwalter im Übrigen unter bestimmten Voraussetzungen auch Rechtshandlungen, die nach Insolvenzeröffnungsantrag noch zur Befriedigung des Gläubigers geführt haben.

Für die Geltendmachung solcher Ansprüche hat der Insolvenzverwalter Zeit; Grenzen sind ihm nur durch die allgemeine Verjährungsfrist gesetzt (drei Jahre nach BGB).

Grundvoraussetzung: Masseverkürzung

Rechtshandlungen sind nur dann anfechtbar, wenn sie im Ergebnis die Masse verkürzt haben, die zur Befriedigung der späteren Insolvenzgläubiger zur Verfügung steht. Eine solche Verkürzung der späteren Insolvenzmasse liegt nicht vor, wenn der späteren Masse bei einem Leistungsaustausch unmittelbar ein Vermögenswert zugeflossen ist, der wertmäßig dem entspricht, was gezahlt worden ist. Das sind die sogenannten Bargeschäfte, bei denen z. B. ein Unternehmer eine Lieferung erbringt und dafür unmittelbar die Zahlung erhält. Wer also von einem Vertragspartner gebeten wird, noch Leistungen zu erbringen in einem Augenblick, in dem er an der wirtschaftlichen Leistungsfähigkeit des Partners schon erhebliche Zweifel hat, kann sich vor späteren Anfechtungen durch Insolvenzverwalter schützen, indem er in Zukunft nur solche Bargeschäfte mit unmittelbarem Leistungsaustausch („Zug-um-Zug“) erbringt.

Wissen kann schaden

Die Insolvenzordnung sieht für Leistungen des späteren Gemeinschuldners in den letzten drei Monaten vor dem Insolvenzeröffnungsantrag verschiedene Anfechtungstatbestände vor.

Sie unterscheidet dabei danach, ob eine Leistung erfolgt ist, auf die ein fälliger Anspruch bestand (kongruente Deckung), oder ob die Leistung erfolgt ist, obwohl in dieser Form oder zu diesem Zeitpunkt noch keine Leistung hätte begehrt werden können (inkongruente Deckung).

Im Falle der kongruenten Deckung kann der Insolvenzverwalter anfechten, wenn der Schuldner im Zeitpunkt der Leistung zahlungsunfähig war und der empfangende Gläubiger die Zahlungsunfähigkeit kannte.

Im Falle der inkongruenten Deckung ist die Anfechtung leichter: Leistungen im Monat vor Eröffnungsantrag können immer angefochten werden, Leistungen im 2. oder 3. Monat vor Eröffnungsantrag, wenn der Schuldner zu dieser Zeit zahlungsunfähig war oder der empfangende Gläubiger wusste, dass diese Zahlung die Insolvenzgläubiger benachteiligte, also die Insolvenzmasse verkürzte.

Soweit es darum geht, ob der empfangende Gläubiger die Zahlungsunfähigkeit kannte oder wusste, dass diese Zahlung die Insolvenzmasse verkürzte, hilft das Gesetz dem Insolvenzverwalter mit Vermutungen. Für die Kenntnis von der Zahlungsunfähigkeit oder der Gläubigerbenachteiligung genügt die Kenntnis der Umstände, die zwingend auf Zahlungsunfähigkeit oder Gläubigerbenachteiligung schließen lassen.

Solche Umstände können sein: Langfristiger Aufbau erheblicher Außenstände, erfolglose Vollstreckungsversuche des Gläubigers, Rückgabe von Lastschriften oder geplatzte Schecks, Nichteinhaltung von gemachten Zahlungszusagen, aussichtslose Vollstreckungsversuche, Gespräche mit dem Schuldner oder Informationen des Schuldners, in denen dieser auf seine drohende Zahlungsunfähigkeit hingewiesen hat.

Gesetzgeber begrenzt Anfechtungsrisiko

Der BGH hatte im Urteil vom 07.05.2020 (IX ZR 18/19) die Gelegenheit, zu einer in die Insolvenzordnung im Jahre 2017 neu eingefügten Bestimmung Stellung zu nehmen, mit der der Gesetzgeber versuchen wollte, das Anfechtungsrisiko zu begrenzen.

Eine Bank hatte einem Gastwirt Kredit gewährt. Der Gastwirt hatte die Ratenzahlungen nicht erbracht. Die Bank hatte den Kredit gekündigt und anschließend mit dem Gastwirt eine Ratenzahlungsvereinbarung zur Kredittilgung geschlossen. Auch diese erfüllte der Gastwirt nur mit wenigen Raten und fiel in Insolvenz.

Der Insolvenzverwalter hat die vom Gastwirt noch geleisteten Raten angefochten, die 6-9 Monate vor Insolvenz-Eröffnungsantrag noch geleistet worden waren. Seine Argumentation: Die Bank habe durch die Zahlungsausfälle und die Kreditkündigung gewusst, dass Zahlungsunfähigkeit des Schuldners drohte und die Zahlung der letzten Raten die Gläubiger benachteiligte.

Nach § 133 InsO sind Leistungen anfechtbar, wenn der leistende Schuldner mit der Absicht handelt, seine Gläubiger zu benachteiligen und der empfangende Gläubiger diesen Vorsatz des Schuldners kennt. Die Kenntnis des empfangenden Gläubigers wird nach dem Gesetz vermutet, wenn er wusste, dass die Zahlungsunfähigkeit des Schuldners drohte bzw. – bei kongruenter Deckung – eingetreten war und dass die Handlung die Gläubiger benachteiligte.

Allerdings: Seit 2017 bekämpft der Gesetzgeber diese Erst-Vermutung mit einer gegenteiligen Zweit-Vermutung im Fall einer kongruenten Deckung: Wenn der Gläubiger mit dem Schuldner (nur) eine Zahlungsvereinbarung getroffen oder ihm in sonstiger Weise eine Zahlungserleichterung gewährt hat, wird vermutet, dass er die Zahlungsunfähigkeit des Schuldners nicht kannte. Allein die Tatsache, dass man mit einem Schuldner eine solche Ratenzahlungsvereinbarung trifft, bedeutet also nicht, dass man deshalb seine Zahlungsunfähigkeit kennt oder von einer Gläubigerbenachteiligung weiß. Allein auf diese Ratenzahlungsvereinbarung kann der Insolvenzverwalter seine Anfechtungsklage also nicht stützen. Wenn er aber beweisen kann, dass dem Gläubiger

noch andere Umstände bekannt waren – aus der Zeit vor einer Ratenzahlungsvereinbarung oder danach – die für eine Zahlungsunfähigkeit des Schuldners sprachen, kann die Anfechtung Erfolg haben.

Wer zu viel über die wirtschaftliche Situation seines Schuldners weiß, den bestraft die Insolvenzordnung – durch Anfechtung erhaltener Leistungen.

Die richtige Taktik wählen

Vor diesem Hintergrund ist, wenn ein Kunde „wackelig" wird, genau abzuwägen, welche Maßnahmen man ergreift, um offene Forderungen noch einzutreiben.

Das Ziel muss sein, für die Vergangenheit eine Regelung zu finden, die jedenfalls Chancen hat, nicht vom Insolvenzverwalter angefochten zu werden. Vor allem aber für die Zukunft bei weiteren Lieferungen eine Regelung zu finden, die anfechtungssicher ist.

Für die Zukunft ist in den meisten Fällen zu empfehlen, an einen solchen wackeligen Kunden nur noch im Rahmen von Bargeschäften zu liefern, also Lieferungen nur zu erbringen, wenn Zug um Zug, spätestens aber im Abstand von 1 bis 2 Wochen nach der Lieferung auch die Zahlung erfolgt.

Wer bei einem wackeligen Kunden bei künftigen Lieferungen auf Bargeschäfte verzichtet, setzt sich einem Anfechtungsrisiko aus.

Für die in der Vergangenheit aufgelaufenen offenen Posten kann man versuchen, eine Regelung zu finden. Wie anfechtungssicher eine solche Regelung, vor allem Zahlungen, die aufgrund einer solchen Regelung dann erfolgen (Ratenzahlungen), ist, hängt entscheidend davon ab, wie die Situation des Schuldners ist und was der Gläubiger darüber erfährt.

Je hoffnungsloser die Situation und je mehr der Gläubiger darüber erfährt, desto schlechter die Chancen, eine anfechtungssichere Regelung zu treffen. Das Risiko von Anfechtungen ist im 3-Monatszeitraum vor Insolvenzeröffnungsantrag besonders hoch.

Dr. Bernhard König
Rechtsanwalt
detmold@brandi.net

Dr. Siegfried Friesen

Gefährdung des Versicherungsschutzes durch kaufvertragliche Abreden

Im Stadium vor dem Abschluss eines Kaufvertrages dürfte das Versicherungsrecht bei den meisten Akteuren eher von untergeordneter Bedeutung sein. Der Fokus ist vielmehr auf das Aushandeln von vertraglichen Vereinbarungen gerichtet mit dem Ziel, die eigene Position zu stärken, mithin die Risiken als Ver- bzw. Käufer auf ein für den Vertragspartner akzeptables Minimum zu reduzieren. Abgesehen von Konstellationen, in denen ein wahrnehmbares Machtgefälle zwischen den Parteien besteht, prägen in der weit überwiegenden Anzahl der Fälle „Geben und Nehmen" die Verhandlungen. So kommt es nicht selten vor, dass eine ungünstige vertragliche Vereinbarung in Kauf genommen wird, im Gegenzug eine andere, günstige, dafür als „Kompensation" Eingang in den Vertrag findet.

Ein Abgleich eines auf diese Weise gemeinsam erarbeiteten Vertrages mit dem Schutz des eigenen, erst recht des gegnerischen Haftpflichtversicherungsvertrages, findet regelmäßig nicht statt. Verkäufer und Käufer gehen schließlich davon aus, dass auf Grundlage eines vorhandenen Versicherungsvertrages ein Deckungsanspruch besteht und sie für den Fall einer Inanspruchnahme etwa auf Schadenersatz gewappnet sind. Als trügerisch erweist sich ein solches Vertrauen, wenn etwa der Käufer Ersatzansprüche geltend macht und diese (auch) deshalb begründet sind, da eine zusätzliche Vereinbarung, die von einer gesetzlichen Vorgabe abweicht, Bestandteil des Vertrages wurde. Ob und in welchem Umfang etwa ein Haftpflichtversicherer leistet, hängt nämlich im Ausgangspunkt davon ab, ob der Versicherungsfall überhaupt eingetreten ist. Dies beurteilt sich im Wesentlichen anhand der entsprechenden Definition innerhalb der Versicherungsbedingungen. Haftpflichtversicherer formulieren hierzu im Kern, dass „Versicherungsschutz besteht […], [wenn] der Versicherungsnehmer […] aufgrund gesetzlicher Haftpflichtbestimmungen privatrechtlichen Inhalts von einem Dritten auf Schadensersatz in Anspruch genommen wird". Mit dieser Formulierung stellt der Versicherer zweierlei klar. Einerseits, dass seine Einstandspflicht besteht, wenn der Versicherungsnehmer auf der Basis des Gesetzes in Anspruch genommen wird und andererseits, dass die Einstandspflicht nur soweit reicht, wie auch die Gesetzeslage es vorsieht.

Hieraus lassen sich folgende Erkenntnisse ableiten. Kommt es allein deshalb zu einer berechtigten Inanspruchnahme, weil vom Gesetz Abweichendes vereinbart wurde, ist der Versicherer vertraglich nicht zur Leistung verpflichtet. Rechtfertigt sich eine Geltendmachung von Forderungen dagegen bereits auf gesetzlicher Grundlage, führen also nicht erst abweichende Vereinbarungen hierzu, bleibt der Versicherer in der Pflicht. Lässt sich die Forderung „aufteilen" (so etwa beim Verzicht auf den Mitverschuldenseinwand, dazu unter 2.), ist der Versicherer (nur) für den von der abweichenden Vereinbarung nicht betroffenen Teil einstandspflichtig.

Auf den ersten Blick liegt es nah, dass etwaige Deckungslücken sich lediglich zum Nachteil des Ersatzpflichtigen auswirken, da dieser ggf. keinen bzw. einen eingeschränkten Versicherungsschutz genießt und damit evtl. mit eigenen Mitteln die Forderung seines Vertragspartners bedienen muss. Bei näherer

Betrachtung fällt indes auf, dass etwaige „Ausfälle des Versicherungsvertrages“ auch den Gläubiger treffen können. Namentlich kommt es auch für ihn zu einer ungünstigen Ausgangslage, wenn die Liquidität des Schuldners eine (vollständige) Schadenskompensation nicht ermöglicht.

Im Zusammenhang mit der aufgezeigten Problematik finden sich diverse Vertragsbedingungen, die oftmals vereinbart werden und ein gewisses „Risikopotential“ beinhalten.

1. Haftungsmodifikationen

Eine Schadenersatzpflicht hängt unter anderem davon ab, dass der Schuldner die Pflichtverletzung – abgesehen von den Fällen der Gefährdungshaftung, etwa nach dem Produkthaftungsgesetz (§ 1 ProdHaftG) – zu vertreten hat (§ 280 BGB). Ob dies der Fall ist, beurteilt sich danach, ob ihm mindestens fahrlässiges Verhalten vorzuwerfen ist (§ 276 BGB).

Vereinbaren die Parteien nun, dass der Schuldner darüber hinaus auch für Zufall haftet oder gar eine Garantieübernahme erklärt, weicht dies von der Gesetzeslage ab, sodass der Versicherer nicht in einer Leistungspflicht steht. Allenfalls ist er einstandspflichtig, wenn der Versicherungsnehmer nachweist, dass seine Haftung gegenüber dem Gläubiger auch auf der Basis der gesetzlichen Bestimmungen besteht.

2. Mitverschuldenseinwand

Ereignet sich auf der Seite des Gläubigers ein Schaden, darf sich dieser nicht untätig zeigen. Er muss vielmehr aufgrund seiner gesetzlichen Obliegenheit (§ 254 BGB) Anstrengungen unternehmen, um den Schaden gering zu halten. Verstößt er hiergegen, berechtigt dieser Umstand den Ersatzpflichtigen zur Kürzung des Anspruchs.

Kann sich der Geschädigte wiederum auf eine vertragliche Vereinbarung berufen, wonach dem Schädiger eine Berufung auf den Mitverschuldenseinwand versperrt ist, ist der Versicherer in Höhe des Mitverschuldens nicht zur Leistung verpflichtet.

3. Rügeobliegenheit

Im kaufmännischen Geschäftsverkehr ist der Käufer gehalten, die gelieferte Ware unverzüglich nach der Ablieferung durch den Verkäufer, soweit dies nach ordnungsmäßigem Geschäftsgange tunlich ist, zu untersuchen und, wenn sich ein Mangel zeigt, dem Verkäufer unverzüglich Anzeige zu machen (§ 377 Abs. 1 HGB). Kommt er dieser Obliegenheit nicht nach, gilt die gelieferte Ware, so wie sie ist, als genehmigt (§ 377 Abs. 2 HGB); Gewährleistungsansprüche kann der Käufer sodann nicht mehr mit Erfolg geltend machen.

Verzichtet der Verkäufer auf den Einwand einer verspäteten Mängelrüge, vermag der Käufer auch im Falle einer Verletzung der aufgeführten Obliegenheit Gewährleistungsansprüche durchzusetzen. In dieser Konstellation droht eine vollständige Deckungslücke, soweit der Rügepflicht rein faktisch hätte nachgekommen werden können aber nicht wurde.

4. Persönliche Haftungserweiterung

Der Schuldner hat für Fehlverhalten seiner Erfüllungsgehilfen einzustehen (§ 278 BGB), worunter wiederum nicht der Hersteller bzw. der Vorlieferant fällt.

Erklärt der Veräußerer im Vertrag, sich Fehlverhalten von sonstigen Dritten zurechnen zu lassen, führt dieser Umstand zu einer Ausweitung auf Pflichten, denen er prinzipiell als Verkäufer nicht nachkommen muss. Schäden, die auf ein solches „freiwillig zugerechnetes“ Fehlverhalten zurückzuführen sind, lösen keine Einstandspflicht des Versicherers aus.

5. Vereinbarungen zur Verjährung

Im Kontext der Verjährung sind diverse vertragliche Vereinbarungen denkbar, die deckungsschädlich sind. Allgemein gilt im Rahmen des Kaufrechts eine 2-jährige Verjährungsfrist, die ab Übergabe der Sache anläuft (§ 438 Abs. 1, 2 BGB). Soll hingegen kraft rechtsgeschäftlicher Abrede die gesetzliche Verjährung maßgeblich sein, verändert sich sowohl der Beginn der Verjährung (§ 199 Abs. 1 BGB) als auch die Dauer (§ 195 BGB), sodass dem Gläubiger ein durchaus erheblich längerer Zeitraum zur Verfügung steht, seine Ansprüche geltend zu machen.

Ferner vermag auch ein Verjährungsverzicht zu einer Deckungsschädlichkeit führen. Eine Ausnahme, wonach eine entsprechende Erklärung die negative Wirkung des fehlenden Versicherungsschutzes nicht nach sich ziehen kann, ist dort zu erblicken, wo ein Verjährungsverzicht die Klageerhebung durch den Gläubiger aus Anlass einer Verjährungshemmung (§ 204 Abs. 1 Nr. 1 BGB) vermeidet; erfolgt die Erklärung in dieser Situation letztlich auch im Interesse des Versicherers.

Mit Vorsicht bleibt weiterhin Vereinbarungen zu begegnen, wonach jede Nacherfüllung durch Neulieferung oder Nachbesserung einen Neubeginn der Verjährung nach sich zieht. Immerhin greift die entsprechende gesetzliche Bestimmung (§ 212 Abs. 1 Nr. 1 BGB) nur, wenn und soweit der Nacherfüllungsanspruch anerkannt wird. Bei reinen Kulanzhandlungen ist dies wiederum nicht der Fall.

Auswirkungen auf den Deckungsumfang scheiden wiederum in den genannten Konstellationen aus, werden Ansprüche innerhalb der vom Gesetz vorgesehenen Verjährungsfrist geltend gemacht.

Es bleibt abschließend zu empfehlen, bei Vertragsverhandlungen stets versicherungsvertragliche Besonderheiten nicht aus dem Blick zu verlieren. Sollten sich bestimmte Vereinbarungen nicht „vermeiden lassen“, so dient eine entsprechende Kontrollüberlegung doch letzten Endes wenigstens dazu, sich die realen wirtschaftlichen Risiken vor Augen zu führen, um diesen sodann auf anderen Wegen zu begegnen.

Dr. Siegfried Friesen
Rechtsanwalt
siegfried.friesen@brandi.net

Christian Rödding

Zwei Jahre Geschäftsgeheimnisgesetz – was hat sich geändert?

Am 26.04.2019 ist das Geschäftsgeheimnisgesetz (GeschGehG) in Kraft getreten. Es dient der Umsetzung einer EU-Richtlinie, durch die der Schutz von Geschäftsgeheimnissen europaweit harmonisiert werden soll.

Das Gesetz hat unmittelbare Auswirkungen darauf, wie Geschäftsgeheimnisse zu schützen sind. Denn während früher – vereinfacht gesprochen – praktisch jede geheime Information, die für den Inhaber von wirtschaftlichem Wert war, auch als Geschäftsgeheimnis geschützt war, muss dieser nun selbst aktiv werden, um seine Geheimnisse zu erhalten.

Denn anders als bisher ist nur noch das nach dem Gesetz als Geschäftsgeheimnis geschützt, was Gegenstand von „nach den Umständen angemessenen Geheimhaltungsmaßnahmen" ist. Eine entsprechende Voraussetzung gab es bisher nicht, sodass hier Prüfungs- und Handlungsbedarf besteht. Was auf den ersten Blick wie eine ohnehin vernünftige Entscheidung klingt, entpuppt sich bei genauerem Hinsehen als gefährliche Stolperfalle. Denn verzichtet der Inhaber von Informationen auf angemessene Maßnahmen zur Geheimhaltung, ist dies fatal: Er hat dann keinerlei rechtlichen Schutz mehr vor Zugriffen auf diese Information, die gegen seinen Willen erfolgen.

Auch nach zwei Jahren ist allerdings noch nicht endgültig geklärt, welche Maßnahmen als „angemessen" gelten. Es muss nicht jede theoretisch denkbare Schutzmaßnahme ergriffen werden – denn jedes Unternehmen hat zwar ein Interesse daran, dass die eigenen Geheimnisse auch geheim bleiben, zu strenge Schutzmaßnahmen sind jedoch weder wirtschaftlich noch verhältnismäßig. Anders ausgedrückt: Es muss stets zwischen den Kosten und dem Nutzen der Maßnahmen abgewogen werden. Nach der Rechtsprechung können hier als Faktoren beispielsweise der Wert des Geschäftsgeheimnisses und dessen Entwicklungskosten, die Natur der Information, die Bedeutung für das Unternehmen, aber auch die Größe des Unternehmens herangezogen werden.

Die Rechtsprechung musste sich bislang nur in wenigen Fällen mit dem neuen Geschäftsgeheimnisgesetz befassen. So hatte das LAG Düsseldorf in seiner Entscheidung vom 03.06.2020 zu prüfen, welche Maßnahmen als „angemessene Geheimhaltungsmaßnahmen" gelten. Ein ehemaliger Arbeitnehmer hatte hier Unterlagen seines früheren Arbeitgebers für seinen neuen Arbeitgeber genutzt, sein früherer Arbeitgeber wollte ihm dies untersagen. In Streit stand hier eine Verschwiegenheitsvereinbarung, die den klagenden Arbeitnehmer zur „absoluten Verschwiegenheit über geheimhaltungsbedürftige Vorgänge" verpflichtete. Das LAG entschied, dass diese Klausel zu weitgehend und damit unwirksam sei. Zudem hatte der Kläger darauf verzichtet, die beim Beklagten verbliebenen Unterlagen herauszufordern und dadurch den Schutz seines „Geheimnisses" noch weiter verwässert (Az.: 12 SaGa 4/20).

Ebenfalls um „angemessene Geheimhaltungsmaßnahmen" ging es in einem Verfahren vor dem OLG Stuttgart. Ein ehemaliger Geschäftsführer und ehemalige Mitarbeiter der Klägerin hatten in einem neuen Unternehmen Rezepturen und chemische Produktionsvorschriften verwendet, die bei der Klägerin zum Einsatz gekommen waren. Diese wollte dies ebenfalls untersagen. Auch hier hatte das Gericht jedoch erhebliche Zweifel am Vorliegen angemessener Schutzmaßnahmen. Insbesondere wurde bemängelt, dass die Klägerin nicht nachgewiesen hatte, die sensiblen Informationen entgegen des „Need-to-know"-Prinzips nur denjenigen zur Verfügung gestellt zu haben, die diese unbedingt für ihre Arbeit benötigten (Az.: 2 U 575/19).

Man sieht: Oftmals scheitert der Geheimnisschutz daran, dass angemessene Maßnahmen nicht ergriffen worden sind.

Was ist nun zu tun?
Es empfiehlt sich dringend, zunächst den aktuellen Status der eigenen Geschäftsgeheimnisse festzustellen, Maßnahmen zu prüfen bzw. zu ergreifen und diese regelmäßig zu aktualisieren. Man sollte sich zunächst einen Überblick darüber verschaffen, um welche Informationen es insoweit geht, welche Personen darauf Zugriff haben und wie die aktuellen Schutzmaßnahmen aussehen. Zur Festlegung, welche – angemessenen – Maßnahmen erforderlich sind, bietet sich sodann eine Einteilung der Geschäftsgeheimnisse in unterschiedliche Kategorien an (existenziell, zentral, sonstige). Je wichtiger ein Geheimnis für das Unternehmen ist, desto stärker muss es geschützt werden.

Die gebotenen Schutzmaßnahmen betreffen sodann im wesentlichen organisatorische Vorkehrungen, die IT-Sicherheit und insbesondere vertragliche Vereinbarungen mit Arbeitnehmern und Geschäftspartnern. Organisatorisch empfiehlt sich die Bestellung eines Geheimschutzbeauftragten. Der Zugang zu Geschäftsgeheimnissen sollte auf das Notwendige begrenzt („Need to know") und Mitarbeiter für Fragen des Geheimnisschutzes sensibilisiert werden. In technischer Hinsicht sollte der Zugang zu Geschäftsgeheimnissen mit personalisierter Benutzerkennung und Passwortschutz ebenso eine Selbstverständlichkeit sein wie die Trennung von beruflich und privat genutzten Geräten. Wichtig sind schließlich geeignete Geheimhaltungsvereinbarungen mit Mitarbeitern und Geschäftspartnern. Hier muss man der Verlockung widerstehen, pauschal jede Information für geheimhaltungsbedürftig zu erklären. Insbesondere bei Vereinbarungen mit Mitarbeitern gelten hohe Wirksamkeitsanforderungen an eine ausreichend bestimmte Regelung, was geheim zu halten ist. Ist eine Geheimhaltungsvereinbarung jedoch zu pauschal oder zu weitgehend, ist sie unwirksam und damit keine Geheimhaltungsmaßnahme mehr. Zur Absicherung der Verpflichtungen des Vertragspartners sind Vertragsstrafenvereinbarungen sinnvoll.

Insbesondere für technische Geschäftsgeheimnisse gibt es eine weitere – entscheidende – Neuerung: Das „Reverse Engineering", also das „Entschlüsseln" von Geheimnissen durch Rückbau von Produkten war früher verboten und ist nun ausdrücklich erlaubt. Auch dadurch besteht eine Gefahr, dass Geheimnisse ohne Konsequenzen aufgedeckt und damit wertlos werden. Es ist allerdings möglich, dies seinem Vertragspartner zu untersagen, was in der Regel auch empfehlenswert sein dürfte.

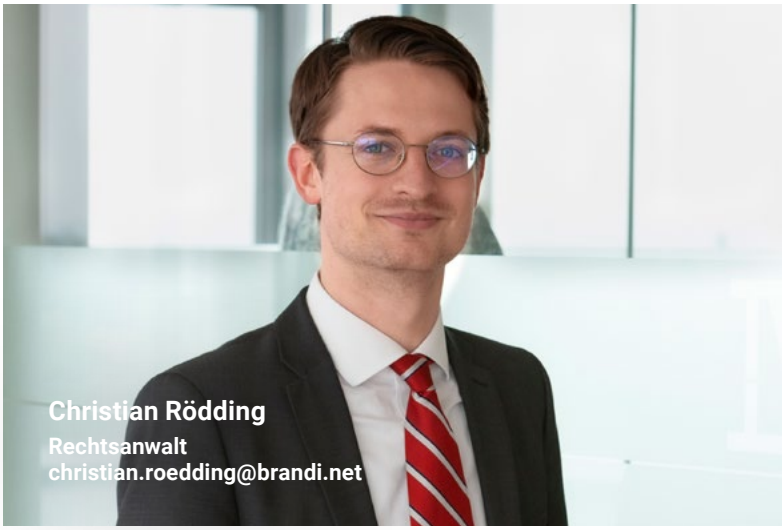
Ausdrücklich geregelt sind nun zudem Ausnahmen, bei denen es erlaubt ist, ein Geschäftsgeheimnis aufzudecken. Dies ist beispielsweise der Fall, bei Ausübung der freien Meinungsäußerung und Informationsfreiheit, Aufdeckung von Missständen zum Schutz des öffentlichen Interesses (sog. Whistleblowing) und

– im begrenzten Umfang – Erfüllung der Aufgaben der Arbeitnehmervertretungen. Inwieweit diese Regelungen den Geheimnisschutz beeinflussen, muss sich noch zeigen.

Wichtig: Nach einer ersten Entscheidung sollen für gerichtliche Verbote im Eilverfahren die wettbewerbsrechtlichen Kriterien entsprechend gelten. Nach Kenntnis von „Ross und Reiter“ eines Gesetzesverstoßes muss ein entsprechender Antrag somit spätestens innerhalb von einem Monat bei Gericht gestellt werden.

Fazit:
Es ist wichtiger denn je, sich um einen angemessenen Geheimnisschutz zu bemühen. Denn solange dieser nicht vorliegt, gibt es kein Geheimnis, was geschützt werden kann – der Betroffene steht dann rechtlich weitgehend schutzlos da. Zwar bleibt im Einzelfall abzuwarten, welche Voraussetzungen die Gerichte an angemessene Schutzmaßnahmen stellen werden; einige Maßnahmen (z. B. wirksame Verschwiegenheitsverpflichtung, „Need-to-know“-Prinzip, technische Zugangsbeschränkungen) sind jedoch unabdingbar.

Darüber hinaus bleibt abzuwarten, wie sich die recht unbestimmten gesetzlichen Verbotsausnahmen (Handeln zum Schutz eines berechtigten Interesses, insbesondere Meinungsfreiheit und Whistleblowing) und der Ausschluss der eigentlich bestehenden Ansprüche bei deren Unverhältnismäßigkeit im Einzelfall in der praktischen Anwendung des Gesetzes auswirken werden. Das gilt auch für die erstmals sehr detailliert geregelten Geheimhaltungsmöglichkeiten der betroffenen Geschäftsgeheimnisse in einem Rechtsstreit.



Christian Rödding
Rechtsanwalt
christian.roedding@brandi.net

Johanna Schmale

Datenschutzrechtstag am 07. Mai 2021

Anlässlich des dreijährigen Jubiläums der Datenschutz-Grundverordnung (DSGVO) hat die BRANDI-Kompetenzgruppe für IT & Datenschutz am 07. Mai 2021 erfolgreich einen Datenschutzrechtstag veranstaltet.

Nachdem zum Inkrafttreten der DSGVO auf einem Datenschutzrechtstag im Jahr 2018 mit verschiedenen Referenten über datenschutzrechtliche Fragen, Risiken und Aussichten diskutiert wurde, konnte auf der diesjährigen Veranstaltung bereits von den bisherigen Erfahrungen mit der DSGVO berichtet werden. Neu war das Format der Veranstaltung: Angesichts der aktuellen Corona-Lage wurde die Veranstaltung als Live-Ereignis online durchgeführt. Über die hohe Teilnehmerzahl und zahlreiche positive Rückmeldungen aus dem Teilnehmerkreis haben wir uns sehr gefreut.

Mit dem rheinland-pfälzischen Datenschutzbeauftragten, Herrn Prof. Dr. Dieter Kugelmann, konnten wir einen renommierten Experten gewinnen, der auf der Veranstaltung einen Einblick in die tägliche Arbeit einer Datenschutzaufsichtsbehörde gegeben hat. Er und seine Gesprächspartner aus unserem Anwaltsbereich, Frau Dr. Laura Schulte, Herr Dr. Sebastian Meyer, Herr Dr. Daniel Wittig und Herr Björn Mai, haben eine spannende Diskussion über Erfahrungen, Probleme und offene Themen bei der täglichen Anwendung der DSGVO geführt, durch die die Moderatoren Herr Dr. Christoph Rempe und Herr Dr. Christoph Worms führten. Herr Björn Mai konnte dabei als Experte des Arbeitsrechts zu den besprochenen Themen wertvolle Hinweise aus der arbeitsrechtlichen Perspektive beisteuern.

Die Veranstaltung war in zwei Blöcke unterteilt: In dem ersten Teil ging es um aktuelle Fragen zum Jubiläum der DSGVO, in dem zweiten Teil um Datenschutz in Unternehmen. Die Zuschauer hatten die Gelegenheit, während der Veranstaltung ihre Fragen an uns zu schicken, sodass diese direkt von den Moderatoren und Referenten in dem Gespräch berücksichtigt werden konnten.

Aktuelle Fragen zum Jubiläum der DSGVO

Herr Prof. Dr. Kugelmann leitete mit einem Impulsvortrag den ersten Teil der Veranstaltung ein, wobei er gleich zu Beginn seine Sichtweise auf die DSGVO darstellte: „Die DSGVO ist ein Erfolg". Dies begründete er damit, dass einerseits die DSGVO als „Exportschlager" dafür gesorgt habe, dass auch außerhalb von Europa über Datenschutz nachgedacht werde und dass andererseits auch in der Wirtschaft angekommen sei, dass es keine Digitalisierung ohne guten Datenschutz gebe.

Er benannte jedoch auch drei Themen, bei denen sich seiner Ansicht nach noch Probleme stellen: Die Datenübermittlung in Drittstaaten, Geldbußen unter der DSGVO sowie datenschutzrechtliche Aspekte der Corona-Pandemie.

Hinsichtlich der Datenübermittlung in Drittstaaten riet er angesichts der Rechtsprechung des Europäischen Gerichtshofs in Sachen „Schrems II" (EuGH, Urt. v. 16.07.2020, Az. C-311/18) dazu, bis zu einer Klärung des Themas, etwa durch die Veröffentlichung neuer Standardvertragsklauseln, die bestehenden Risiken durch Schutzmaßnahmen so weit wie möglich zu minimieren – je geringer das Risiko eines Datenschutzverstoßes sei, desto eher könne eine Datenübermittlung stattfinden.

Bei der Verhängung von Bußgeldern könne sich eine Datenschutz-Aufsichtsbehörde nach seiner Auffassung unmittelbar an eine juristische Person wenden. Anderslautende Regelungen des deutschen Rechts, nach denen zunächst ein Organisationsverschulden eines Geschäftsführers nachgewiesen werden müsse, seien insofern unanwendbar. Dafür spreche die effektive Durchsetzung des Europarechts, da die konkrete Verantwortlichkeit für einen Datenschutzverstoß regelmäßig nur schwer nachgewiesen werden könne. Herr Prof. Dr. Kugelmann wies jedoch auch darauf hin, dass unterschiedliche Landgerichte diesbezüglich in der Vergangenheit verschiedene Auffassungen vertreten haben.

Zu dem Thema „Datenschutz und Corona" stellte er in seinem Vortrag fest, dass der Datenschutz die Pandemiebekämpfung nicht verhindere.

Die von Herrn Prof. Dr. Kugelmann aufgeworfenen Themen wurden in dem anschließenden Gespräch zusammen mit den weiteren Referenten diskutiert. Zu der Frage der Moderatoren, ob die DSGVO eine Bremse sei, beleuchtete Herr Dr. Meyer die Unternehmenssicht. Positiv an der DSGVO sei, dass für europaweit tätige Unternehmen nicht mehr die Unsicherheiten aufgrund unterschiedlicher rechtlicher Bewertungen in verschiedenen europäischen Staaten bestünden. Unternehmen würden sich durch die DSGVO aber auch neuen Anforderungen stellen, die möglicherweise als bremsend empfunden würden. In der Entstehungsgeschichte der DSGVO seien deren Hauptadressaten ursprünglich große internationale Konzerne gewesen. Von kleinen und mittleren Unternehmen werde es häufig als Hindernis wahrgenommen, dass sie die hohen Anforderungen mit ihrem kleineren Budget erfüllen müssen, dass eine übergeordnete Klärung der Themen mit den großen Anbietern aber nicht erfolge.

Für besonders viele Rückmeldungen aus dem Publikum sorgte in dem Zusammenhang eine Diskussion über den Einsatz von Videokonferenz-Tools amerikanischer Anbieter. Herr Prof. Dr. Kugelmann wies darauf hin, dass es sich zwar um amerikanische Anbieter, aber deutsche Nutzer handele. Ansprechpartner für die Behörde seien diejenigen, die vor Ort für die Datenverarbeitung verantwortlich seien. Unternehmen müssten prüfen, ob es alternative Anbieter in der EU gebe. Die Datenschutz-Aufsichtsbehörde Rheinland-Pfalz empfehle etwa für Schulen das Tool Big Blue Button, toleriere aber aktuell für eine gewisse Übergangszeit noch Microsoft Teams und Zoom. Eine Abschottung der Europäer von der Digitalisierung durch die strengen Datenschutzregelungen sehe er nicht.

Herr Dr. Wittig bemerkte dazu, dass es beispielsweise für Office 365 für viele Unternehmen keine geeignete Alternative aus Europa gebe. Herr Dr. Meyer ergänzte, dass für den Fall, in dem keine Alternative gefunden werden könne, eine klare Kommunikation der Folgen erwartet werde: Entweder werde versucht, das Problem mit den Anbietern in den USA zu klären, wobei bis zur Klärung die Nutzung der amerikanischen Tools toleriert werde, oder es werde ein Verbot ausgesprochen und durchgesetzt.

Zu großen Teilen einig waren sich die Referenten darüber, dass es das Anliegen der DSGVO sein müsse, auch über die euro-

„BRANDI MACHT MOBIL“

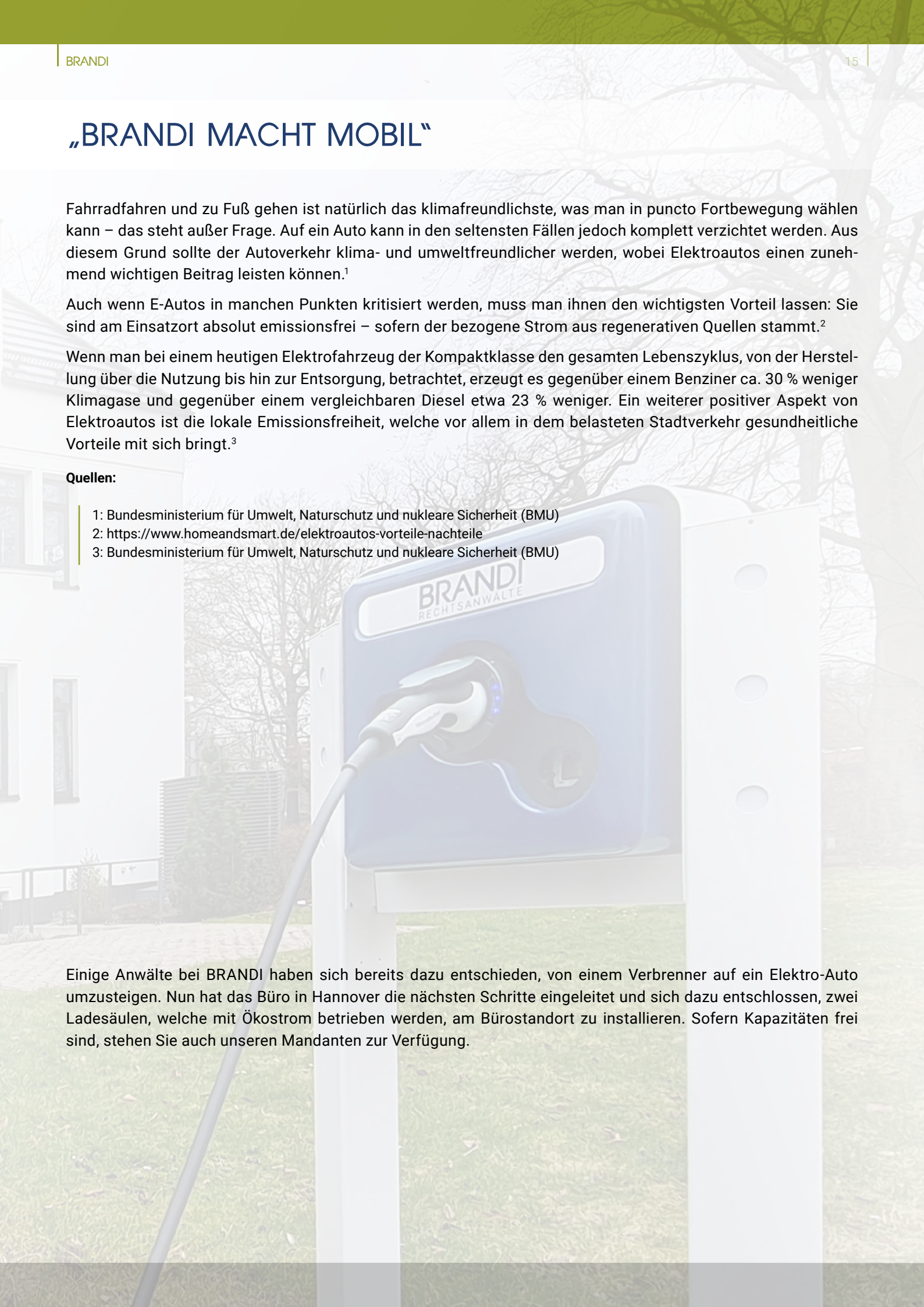
Fahrradfahren und zu Fuß gehen ist natürlich das klimafreundlichste, was man in puncto Fortbewegung wählen kann – das steht außer Frage. Auf ein Auto kann in den seltensten Fällen jedoch komplett verzichtet werden. Aus diesem Grund sollte der Autoverkehr klima- und umweltfreundlicher werden, wobei Elektroautos einen zunehmend wichtigen Beitrag leisten können.[1]

Auch wenn E-Autos in manchen Punkten kritisiert werden, muss man ihnen den wichtigsten Vorteil lassen: Sie sind am Einsatzort absolut emissionsfrei – sofern der bezogene Strom aus regenerativen Quellen stammt.[2]

Wenn man bei einem heutigen Elektrofahrzeug der Kompaktklasse den gesamten Lebenszyklus, von der Herstellung über die Nutzung bis hin zur Entsorgung, betrachtet, erzeugt es gegenüber einem Benziner ca. 30 % weniger Klimagase und gegenüber einem vergleichbaren Diesel etwa 23 % weniger. Ein weiterer positiver Aspekt von Elektroautos ist die lokale Emissionsfreiheit, welche vor allem in dem belasteten Stadtverkehr gesundheitliche Vorteile mit sich bringt.[3]

Quellen:

1: Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit (BMU)
2: https://www.homeandsmart.de/elektroautos-vorteile-nachteile
3: Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit (BMU)



Einige Anwälte bei BRANDI haben sich bereits dazu entschieden, von einem Verbrenner auf ein Elektro-Auto umzusteigen. Nun hat das Büro in Hannover die nächsten Schritte eingeleitet und sich dazu entschlossen, zwei Ladesäulen, welche mit Ökostrom betrieben werden, am Bürostandort zu installieren. Sofern Kapazitäten frei sind, stehen Sie auch unseren Mandanten zur Verfügung.

päischen Grenzen hinaus den Datenschutzstandard der EU zu exportieren. Soweit es alternative Anbieter in der EU gebe, solle der europäische Datenschutz erreichen, dass diese von den Nutzern in den Blick genommen werden. In der Übergangszeit, in der rechtliche Unsicherheiten bestehen, sei eine gewisse Toleranz für die Nutzung von Anbietern in Drittstaaten gefordert.

Zu der Frage, ob die DSGVO ein Unsicherheitsfaktor sei, erläuterte Herr Dr. Meyer, dass die DSGVO Grundprinzipien und Kriterien zur Orientierung aufstelle, jedoch nicht jeden Einzelfall regeln könne. Der Ansatz der DSGVO sei gerade ein risikobasierter, sodass in jedem Einzelfall der Sachverhalt unter die Normen der DSGVO subsumiert werden, eine Risikobewertung erfolgen und die Frage nach den Absicherungsmöglichkeiten gestellt werden müsse.

Herr Prof. Dr. Kugelmann stimmte dem zu und ergänzte, dass die DSGVO ein rechtskonformes Verhalten zum Ziel habe. Dementsprechend sollten Bußgelder abschreckend wirken.

Bei der Frage nach dem Schmerzensgeld für Datenschutzverstöße sagten Herr Prof. Dr. Kugelmann und Herr Dr. Meyer übereinstimmend, dass auch vermeintlich missbräuchliche Auskunftsansprüche zunächst neutral behandelt werden müssten. Herr Dr. Meyer ergänzte, dass jedoch die massenhafte Geltendmachung von Auskunftsansprüchen mit Hilfe von Fremddienstleistern die Frage aufwerfe, ob nicht insofern eine stärkere Missbrauchskontrolle erforderlich sei. Hierüber müsse möglicherweise zukünftig politisch nachgedacht werden.

Datenschutz im Unternehmen

Der zweite Teil der Veranstaltung begann mit einem Impulsvortrag zum Thema „Datenschutz im Unternehmen" von Frau Dr. Schulte. Dabei ging sie auf verschiedene Anwendungsszenarien ein, in denen sich in Unternehmen datenschutzrechtliche Probleme stellen. Direkt zu Beginn ihres Vortrags stellte Frau Dr. Schulte heraus, dass die datenschutzrechtlichen Grundsätze auch unter den Bedingungen der Corona-Pandemie zu wahren seien. Anerkannt sei zudem eine gewisse Schutzbedürftigkeit des Arbeitnehmers, die sich auch auf das Datenschutzrecht auswirke. Corona-Testergebnisse seien Gesundheitsdaten, für die eine besondere Schutzbedürftigkeit bestehe.

Zum Arbeiten im Homeoffice stellte Frau Dr. Schulte fest, dass hierbei grundsätzlich ein gegenüber dem Arbeiten im Unternehmen erhöhtes Risiko für den Schutz personenbezogener Daten bestehe. Der Arbeitgeber habe aber dennoch die Pflicht, den Schutz der Daten zu gewährleisten. Zu diesem Zweck empfahl sie Homeoffice-Vereinbarungen, transparente Datenschutzinformationen sowie die Absicherung durch technische und organisatorische Maßnahmen.

In der anschließenden Diskussion wurde zunächst über die Rolle des Betriebsrats gesprochen, wobei Herr Prof. Dr. Kugelmann die umstrittene Frage, ob es eine eigene datenschutzrechtliche Verpflichtung des Betriebsrats gebe, verneinte und erläuterte, er sehe vielmehr die Verantwortlichkeit des Arbeitgebers. In dem Fall, in dem der Betriebsrat seine Zustimmung zu der Einführung von bestimmten technischen und organisatorischen Maßnahmen zur Einhaltung des Datenschutzes, beispielsweise einer Zugangskontrolle, verweigere und deshalb eine Einigungsstelle bemüht werde, komme es letztlich auf den Einzelfall an, ob die Verweigerung der Zustimmung als Entschuldigung gegenüber der Aufsichtsbehörde dienen könne. Grundsätzlich tendiere er dazu, die Rechtsmaterien nicht gegeneinander auszuspielen, sondern zunächst das Ergebnis der Einigungsstelle abzuwarten.

Im Zusammenhang mit dem Thema „Corona und Datenschutz" wurde die Frage diskutiert, welche personenbezogenen Daten der Arbeitnehmer insofern von dem Arbeitgeber erhoben werden dürfen. Nach Auffassung von Herrn Mai dürfe der Arbeitgeber den Arbeitnehmer nur dann nach dessen Impfpass fragen, wenn es eine von dem Arbeitgeber begründete Impflicht gebe. Nur in dem Fall einer solchen Impflicht könne auch ein Interesse des Arbeitgebers bestehen, eine Impfung nachgewiesen zu bekommen. Herr Prof. Dr. Kugelmann ergänzte hierzu, das Datenschutzrecht würde dem Arbeitsrecht insofern folgen; es sei letztlich auch eine Frage nach der Erforderlichkeit, Begründung und Nachvollziehbarkeit, ob eine entsprechende Datenverarbeitung zulässig sei.

Bezüglich der Dokumentation von Testergebnissen wies Frau Dr. Schulte darauf hin, dass die landesrechtlichen Corona-Schutzverordnungen unterschiedliche Dokumentationspflichten vorsehen. Wenn eine Dokumentation gesetzlich nicht zwingend vorgeschrieben sei, sondern nur ein Testangebot vorgehalten werden müsse, sei eine darüberhinausgehende Dokumentation datenschutzrechtlich problematisch; als Rechtsgrundlage könne eine gesetzliche Erlaubnis insofern nicht herangezogen werden. Dies gelte auch für den Fall, dass der Arbeitgeber Zweifel an der ordnungsgemäßen Durchführung der Tests durch die Arbeitnehmer habe. Bei einem positiven Testergebnis sehe der Gesetzgeber Verhaltenspflichten für den Getesteten vor, in die der Gesetzgeber den Arbeitgeber gerade nicht integriert habe. Herr Prof. Dr. Kugelmann stimmte dem zu und ergänzte: „Ein Grundmisstrauen gegenüber dem Arbeitnehmer ist keine datenschutzrechtliche Kategorie".

Die angeregte Diskussion während der Veranstaltung zeigte, dass aktuell, unter anderem aufgrund der Corona-Pandemie und der Rechtsprechung zu Datenübermittlungen in Drittstaaten, verschiedene datenschutzrechtliche Themen an Bedeutung gewonnen haben und für rechtliche Unsicherheiten sorgen. Mitschnitte aus der Veranstaltung finden Sie auf unserer Homepage unter „Veranstaltungen" oder als Podcast unter „News/Podcast".

Johanna Schmale
Wissenschaftliche Mitarbeiterin
johanna.schmale@brandi.net

Dr. Sebastian Meyer, LL.M.

Bußgelder für Datenschutzverstöße – Update 2021

Seit Einführung der neuen Regelungen zur Bußgeldbemessung bei Datenschutzverstößen in der Datenschutz-Grundverordnung (DSGVO) machte es bisweilen den Eindruck, die Aufsichtsbehörden wollten sich immer weiter im Hinblick auf die Höhe der festgesetzten Bußgelder überbieten. Der formale Rahmen für die Bußgeldbemessung in Art. 83 DSGVO sieht lediglich zwei Stufen vor, und zwar Bußgelder bis zu 10 Mio. Euro bzw. bis zu 20 Mio. Euro. Die entsprechenden Werte lassen sich nur vor dem Hintergrund der Entstehungsgeschichte der DSGVO erklären. Es sollte durch die Wahl der hohen Werte im Sinne einer Symbolpolitik verdeutlicht werden, dass Datenschutz zukünftig einen höheren Stellenwert einnehmen muss und Verstöße gravierende Konsequenzen haben können.

Angesichts der in der DSGVO verankerten Grundkonzeption, die Größe eines Unternehmens – oftmals auch bewertet auf der Basis des erreichten Umsatzes – als einen relevanten Faktor bei der Bußgeldbemessung heranzuziehen, war es nicht besonders überraschend, dass die Datenschutzkonferenz als Zusammenschluss der deutschen Aufsichtsbehörden in ihrem Konzept zur Bußgeldbemessung einen wirtschaftlichen Grundwert als Ausgangspunkt für die Bestimmung des konkreten Bußgeldes heranzieht, der sich alleine daran orientiert, welchen Umsatz das betroffene Unternehmen zuletzt erzielt hat. Abhängig von der Schwere des Verstoßes und sonstigen Rahmenbedingungen wird dann der wirtschaftliche Grundwert mit einem Faktor von 1 bis 12 multipliziert. Es liegt auf der Hand, dass sich bei dieser Herangehensweise konkrete Werte für Bußgelder ergeben, die auf den ersten Blick präzise mathematisch hergeleitet sind, sich aber kaum als angemessen und sachgerecht erklären lassen. Nicht ohne Grund verzichtet die Regelung in Art. 83 DSGVO, die europaweit den Bußgeldrahmen definiert, auf eine genaue Gewichtung einzelner Aspekte und verlangt nur allgemein, dass Bußgelder wirksam, verhältnismäßig und abschreckend sein sollen. Dieser Dreiklang aus Wirksamkeit, Verhältnismäßigkeit und Abschreckung ist zuletzt sehr in den Hintergrund geraten, da extrem einseitig vor allem eine Konzentration auf die Abschreckung erfolgt ist. Mittlerweile liegen aber erste Entscheidungen der Instanzgerichte vor, die sich kritisch mit der Anwendung der Bußgeldregelungen aus der DSGVO befassen und zumindest einige Exzesse bei der Bußgeldbemessung korrigieren.

Bußgeldpraxis in Deutschland und Europa

Die Bußgeldpraxis der Aufsichtsbehörden in Deutschland ist dabei im europäischen Vergleich zunächst noch vergleichsweise moderat. Die Mehrzahl der verhängten Bußgelder fällt aktuell noch entsprechend aus; kontrovers diskutiert wird natürlich vor allem über einige wenige Einzelfälle mit besonders hohen Bußgeldern. Lange Zeit war Spitzenreiter in Deutschland das Immobilienunternehmen Deutsche Wohnen, von dem die Aufsichtsbehörde in Berlin 14,5 Mio. Euro für die nicht ordnungsgemäße Datenlöschung verlangte. Zuletzt übernahm das Modeunternehmen H&M den Spitzenplatz mit einem Bußgeld über 35 Mio. Euro für die systematische Erstellung von Mitarbeiterprofilen unter Verstoß gegen datenschutzrechtliche Vorgaben. Relativ hoch fiel auch das Bußgeld der Aufsichtsbehörde aus Niedersachsen gegen den Elektronikhändler notebooksbilliger aus, der 10,4 Mio. Euro für eine unzulässige Videoüberwachung zahlen soll.

In Frankreich hat die Aufsichtsbehörde CNIL sich sehr intensiv mit den Aktivitäten von Google befasst und bereits mehrfach Bußgelder verhängt. Zuletzt verlangte die CNIL im Dezember 2020 von dem Google-Konzern insgesamt 100 Mio. Euro für den nicht rechtskonformen Einsatz von Tracking-Cookies sowie mangelhafte Datenschutzinformationen. Zwischenzeitlich hatte die englische Aufsichtsbehörde ICO angekündigt, die Hotelkette Marriott auf Basis der DSGVO mit einem Bußgeld von mehr als 100 Mio. Euro für den nicht ausreichenden Schutz ihrer zentralen Kundendatenbank belegen zu wollen, was das höchste bisher festgesetzte Bußgeld für Datenschutzverstöße in Europa gewesen wäre. Tatsächlich hat das ICO aber von sich aus unter Berücksichtigung der Stellungnahme von Marriott das Bußgeld letztlich auf 18 Mio. GBP reduziert.

Gerichtliche Überprüfung der Bußgelder

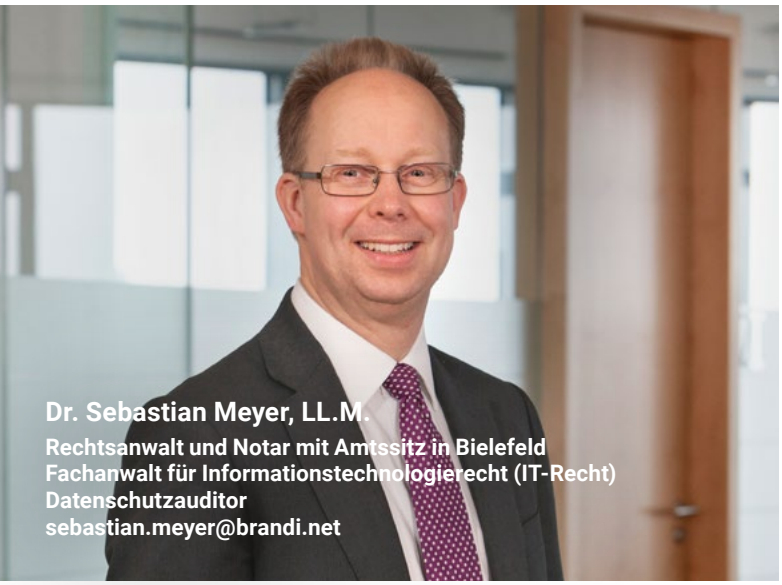
Es war eigentlich nur eine Frage der Zeit, bis die ersten Gerichte sich kritisch mit dem Bußgeldkonzept der Datenschutzkonferenz auseinandersetzen und jedenfalls die Bußgeldhöhe auf ein vernünftiges Maß zurückstutzen. Das Landgericht Bonn musste sich mit dem Bußgeldbescheid des Bundesdatenschutzbeauftragten gegen 1&1 befassen, den 1&1 – wenig überraschend – nicht akzeptieren wollte. Im November 2020 wurde das Vorliegen eines sanktionierungswürdigen Datenschutzverstoßes zwar dem Grunde nach bestätigt, zugleich aber das Bußgeld von 9,5 Mio. Euro auf 900.000 Euro und damit auf weniger als ein Zehntel reduziert (LG Bonn, Urt. v. 11.11.2020, Az. 29 OWi 1/20). In der Entscheidung stellt das Gericht – völlig zu Recht – darauf ab, dass die verschiedenen Zumessungskriterien „in jedem Einzelfall gebührend zu berücksichtigen sind“. Diese Klarstellung kann dabei als berechtigte generelle Kritik an dem gesamten Konzept zur Bußgeldbemessung der Datenschutzkonferenz verstanden werden. Zutreffend verweist das Gericht darauf, dass sich vor allem unpassende Ergebnisse bei schweren Verstößen umsatzschwacher Unternehmen sowie bei leichten Verstößen umsatzstarker Unternehmen ergeben. Generell stellt das Bußgeldkonzept zu einseitig auf den Umsatz eines Unternehmens ab, wenn ausschließlich hiervon der wirtschaftliche Grundwert abhängig ist. Wie eine sinnvolle Berücksichtigung des Umsatzes als ein möglicher Faktor dagegen hätte aussehen können, zeigt die Argumentation des LG Bonn, das ausgehend von den Kriterien der Wirksamkeit und Angemessenheit gem. Art. 83 DSGVO Überlegungen zur „Ahndungsempfindlichkeit“ von Unternehmen anstellt. Im Ergebnis hat das LG Bonn sich vollkommen von der Herleitung der Bußgeldhöhe durch den Bundesdatenschutzbeauftragten gelöst und nach eigenem Ermessen ohne Formelwerk einen Betrag in Höhe von 900.000 Euro festgesetzt. Das Gericht führt dabei zahlreiche Aspekte auf, die eine Bewertung als „minderschweren Fall“ rechtfertigen.

Noch weiter geht das Landgericht Berlin, dass das Bußgeld der Aufsichtsbehörde gegen die Deutsche Wohnen insgesamt wegen „gravierender Mängel“ als unwirksam erklärt und das Verfahren eingestellt hat (LG Berlin, Beschl. v. 18.02.2021, Az. 212 Js-OWi 1/20). Das Gericht störte sich insbesondere daran, dass die Aufsichtsbehörde nicht dargetan hätte, an welche schuldhafte Handlung angeknüpft werden soll. Tatsächlich sieht das Konzept der DSGVO kein Verschuldenserfordernis vor, sondern stellt alleine auf einen objektiven Verstoß gegen datenschutzrechtliche Vorgaben ab. Jedenfalls für das Landgericht ist es aber aus verfassungsrechtlichen Grundsätzen ausgeschlossen, dass in Deutschland ein Unternehmen ein Bußgeld zahlen muss,

ohne dass Grundlage hierfür ein schuldhaftes Verhalten einer einzelnen Person wäre. Auf Wunsch der Aufsichtsbehörde hat die Staatsanwaltschaft gegen die Verfahrenseinstellung Rechtsmittel eingelegt, so dass sich das Kammergericht in nächster Instanz mit der Sache befassen muss.

Das gegen H&M verhängte Bußgeld ist dagegen zwischenzeitlich bestandskräftig geworden, allerdings hatte dort H&M auch auf eine gerichtliche Überprüfung verzichtet.

Fazit
Unter Berücksichtigung des Ergebnisses der gerichtlichen Überprüfung der Bußgelder gegen 1&1 sowie die Deutsche Wohnen zeigt sich trotz der unterschiedlichen Begründungen, dass es in der aktuellen Situation durchaus lohnen dürfte, im Falle der Verhängung von Bußgeldern gegen entsprechende Bescheide auch gerichtlich vorzugehen. Noch sinnvoller ist es aber natürlich, intern ein Datenschutzmanagementsystem zu etablieren, dass Datenschutzverstöße nach Möglichkeit verhindert und – sollte gleichwohl ein Datenschutzverstoß auftreten – im Idealfall eine Verständigung mit der zuständigen Aufsichtsbehörde zu erreichen.



Dr. Sebastian Meyer, LL.M.
Rechtsanwalt und Notar mit Amtssitz in Bielefeld
Fachanwalt für Informationstechnologierecht (IT-Recht)
Datenschutzauditor
sebastian.meyer@brandi.net

Robert Bommel, LL.M.

Schmerzensgeld für Datenschutzverstöße – Aktuelle gerichtliche Entscheidungen und Entwicklungen

Unternehmen können auf Schmerzensgeld verklagt werden, wenn sie gegen das Datenschutzrecht verstoßen. Anders als im alten Datenschutzrecht sieht die Datenschutzgrundverordnung (DSGVO) einen entsprechenden sog. „immateriellen" Schadensersatzanspruch, also einen Anspruch auf Schmerzensgeld, in Art. 82 DSGVO ausdrücklich vor. Doch in welchen Fällen wird Betroffenen tatsächlich ein Schadensersatzanspruch zugesprochen und wie ist der „Schmerz" bei Datenschutzverletzungen summenmäßig zu beziffern? Höchstrichterliche Entscheidungen zu diesem Thema liegen bisher nicht vor. Es lohnt sich aber, einen Blick auf die Rechtsprechung der unteren Instanzgerichte zu werfen.

Das Amtsgericht Hildesheim verurteile ein Computerfachgeschäft zur Zahlung von 800 Euro Schmerzensgeld, weil dieses vor dem Weiterverkauf eines als Mangelware zurückgesandten Rechners nicht die darauf noch zu findenden personenbezogenen Daten des Kunden gelöscht hatte (AG Hildesheim, Urt. V. 05.10.2020, Az. 43 C 145/19). Das Landgericht Lüneburg entschied, dass eine Bank für eine unberechtigte Schufa-Meldung 1.000 Euro Schmerzensgeld zahlen muss (LG Lüneburg, Urt. V. 14.07.2020, Az. 9 O 145/19). Deutlich restriktiver bei der Auslegung der DSGVO war das Landgericht Köln. Dieses verneinte einen Anspruch auf Schadensersatz gegen die Hausbank des Klägers wegen einer einmaligen Falschzusendung von Kontoauszügen an einen Dritten. Dies sei für den Kläger eine bloße Unannehmlichkeit, aber kein zivilrechtlicher Schaden. Der Kläger hatte erfolglos 25.000 Euro Schmerzensgeld beantragt (LG Köln, Urt. v. 7.10.2020, Az. 28 O 71/20). Die Gerichte der ersten Instanzen legen die Vorschriften der DSGVO also durchaus unterschiedlich aus.

Von besonderer Relevanz für Unternehmen ist die Tatsache, dass nicht nur Kunden, sondern auch Arbeitnehmer auf datenschutzrechtliches Schmerzensgeld klagen können. Das Arbeitsgericht Lübeck ging im Fall einer unterbliebenen Löschung von Fotos eines (zwischenzeitlich ausgeschiedenen) Mitarbeiters auf dem Facebook-Account eines Unternehmens von einem Datenschutzverstoß des Unternehmens aus und bezifferte den Streitwert auf 1.000 Euro (ArbG Lübeck, Beschl. v. 20.6.2019, Az. 1 Ca 538/19). Das LG Darmstadt sprach einem Kläger ein Schmerzensgeld von 1.000 Euro zu, weil dessen Bewerbung von einem Unternehmen irrtümlich an einen Dritten beim Karrierenetzwerk Xing weitergeleitet worden war (LG Darmstadt, Urt. v. 26.05.2020, Az. 13 O 244/19).

Die gute Nachricht: Jedenfalls für die Frage nach Schmerzensgeld beim unberechtigten Versand von Werbe-E-Mails steht nun eine höchstrichterliche Klärung in Aussicht. Der Fall: Ein Anwalt verlangte 500 Euro Schmerzensgeld für eine datenschutzwidrig an ihn versandte Werbe-E-Mail. Das Amtsgericht Goslar lehnte den Anspruch des Klägers mit der Begründung ab, es handle sich nur um einen unerheblichen Verstoß, da nur eine einzige unerlaubte E-Mail versandt worden sei (AG Goslar, Urt. v. 27.09.2019, Az. 28 C 7/19). Der Kläger erhob daraufhin Verfassungsbeschwerde vor dem Bundesverwaltungsgericht, die er gewann (BVerfG, Beschl. v. 14.01.2021, Az. 1 BvR 2853/19). Das Bundesverfassungsgericht stellte fest, dass die Frage der Erheblichkeit von Datenschutzverstößen zur Begründung von Schadensersatzforderungen eine Auslegung der Vorschriften der DSGVO erforderlich macht. Hierfür sei aber der Europäische Gerichtshof (EuGH) zuständig. Das AG Goslar hätte also den Anspruch des Klägers nicht einfach ablehnen dürfen, sondern hätte zuvor den EuGH zur Auslegung der einschlägigen Datenschutznormen befragen müssen. Das Verfahren wurde an das AG Goslar zurückverwiesen und wird nun erwartungsgemäß von dort aus dem EuGH vorgelegt werden. Es wird das erste Mal sein, dass der EuGH vertieft zu Fragen eines Schmerzensgelds nach der DSGVO Stellung nehmen wird. Mit einem Urteil des EuGHs ist aber voraussichtlich nicht vor Ende 2022 zu rechnen.

In der Zwischenzeit verbleibt die problematische Situation einer stark divergierenden Rechtsprechung. Unternehmen sollten sich insoweit datenschutzrechtlich gut aufstellen und mit der Rechtsprechung in ihrem Gerichtsbezirk vertraut machen.

Robert Bommel, LL.M.
Wissenschaftlicher Mitarbeiter
robert.bommel@brandi.net

Dr. Laura Schulte

Digitale Inhalte und Dienstleistungen – Die neue Rechtslage

Breits im Jahr 2019 ist auf europäischer Ebene die Richtlinie (EU) 2019/770 über bestimmte vertragliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen (im Folgenden „DID-RL") in Kraft getreten. Die DID-RL soll sowohl der Verbesserung des Verbraucherschutzes als auch des grenzüberschreitenden elektronischen Handelsverkehrs innerhalb der Europäischen Union dienen. Der Rechtsakt enthält insbesondere Regelungen über die Soll-Beschaffenheit sowie Gewährleistungsrechte, speziell in Bezug auf digitale Produkte. Obwohl der Rechtsakt – trotz dem nahenden Ende der Umsetzungsfrist am 1. Juli 2021 – noch nicht verbindlich in nationales Recht transformiert wurde, ist aufgrund des Gesetzesentwurfs der Bundesregierung vom 17. März 2021 (BT-Drs. 19/27653) bereits absehbar, dass mit der Umsetzung der Richtlinie eine umfangreiche Ergänzung des BGB verbunden sein wird.

Anwendungsbereich

Der Anwendungsbereich der DID-RL erfasst grundsätzlich sämtliche Verträge, auf deren Grundlage Unternehmer Verbrauchern digitale Dienstleistungen entgeltlich bereitstellen. Als Entgelt erkennt die Richtlinie neben etablierten Zahlungsmitteln nunmehr auch die Zurverfügungstellung von personenbezogenen Daten, die nicht bereits für die Bereitstellung des Inhalts bzw. des Dienstes erforderlich sind, an, vgl. Art. 3 Abs. 1 DID-RL. Damit trägt der Europäische Gesetzgeber dem Umstand Rechnung, dass personenbezogene Daten zunehmend intensiver kommerzialisiert werden.

Digitale Inhalte oder Dienstleistungen werden künftig unter dem Oberbegriff „digitale Produkte" zusammengefasst. Unter diesem Begriff können etwa Computerprogramme, Video-, Audio- und Musikdateien und elektronische Bücher gefasst werden. Weiterhin können Cloud- und Software „as a Service"-Dienste als digitale Dienstleistungen qualifiziert werden.

Einzelne Regelungen im Überblick

Mit der Einführung der Kategorie des digitalen Produkts wird in Umsetzung der DID-RL der Begriff der „Vertragsgemäßheit" als neuartiger Begriff zur Bestimmung der Soll-Beschaffenheit digitaler Produkte in das BGB eingeführt. Ein digitales Produkt ist hiernach vertragsgemäß, wenn es sowohl verschiedene objektive als auch subjektive Kriterien erfüllt. Die subjektive Vertragsgemäßheit zielt auf die Anforderungen ab, die sich konkret aus dem zwischen Unternehmer und Verbraucher im Hinblick auf das Produkt bestehenden Vertrag ergeben. Zunächst erscheint es wenig überraschend, dass ein Produkt den zugrundeliegenden vertraglichen Bestimmungen entsprechen muss, um als mangelfrei bzw. vertragsgemäß gelten zu können. Allerdings dürfte aus dieser Anforderung in Kombination mit den weiteren Verbraucherschutzregelungen der Richtlinie, etwa zur Haftung des Unternehmers (Art. 9 DID-RL), zur Beweislastumkehr (Art. 12 DID-RL) und den Gewährleistungsrechten des Verbrauchers (u. a. Art. 14 DID-RL), ein nicht unerheblicher Aufwand bei der (Neu-)Gestaltung von Verbraucherverträgen für Unternehmer zur Abbildung der neuen Gesetzeslage resultieren. Vergleichbares gilt für die Realisierung der nunmehr bestehenden Aktualisierungspflichten bzw. Pflichten zur Bereitstellung von Sicherheits-Updates im Hinblick auf digitale Produkte (Art. 8 Abs. 2 DID-RL).

Schließlich plant der nationale Gesetzgeber die Bestimmungen über digitale Produkte im Rahmen einer Änderung des Unterlassungsklagegesetzes (UKlaG) ausdrücklich als Verbraucherschutzgesetze zu qualifizieren, deren Verletzung damit nicht nur die betroffenen Verbraucher selbst, sondern auch qualifizierte Einrichtungen i. S. d. UKlaG geltend machen können.

Fazit

In Umsetzung der Richtlinie über digitale Produkte werden das BGB, das EGBGB und das UKlaG spätestens mit Wirkung zum 1. Januar 2022 reformiert. Die gesteigerten Verbraucherschutzanforderungen werden für Unternehmer mit einem nicht unerheblichen Umsetzungsaufwand verbunden sein. Vor allem bei der Gestaltung von Verbraucherverträgen, aber insbesondere auch der Konzeption, Bewerbung, Kennzeichnung und Zurverfügungstellung digitaler Produkte, werden Unternehmer künftig in eigenem Interesse gehalten sein, den Leistungsumfang digitaler Produkte hinreichend präzise und differenziert zu formulieren. Dies gilt umso mehr angesichts der strengen Wirksamkeitsanforderungen, die an Allgemeine Geschäftsbedingungen gestellt werden und auch in diesem Kontext Relevanz entfalten.

Dr. Laura Schulte
Rechtsanwältin
laura.schulte@brandi.net

Dr. Christoph Rempe

Veröffentlichung eines Fotos auf der Facebook-Fanpage

Das Oberverwaltungsgericht Lüneburg hat in einem Verfahren über eine Verwarnung der Niedersächsischen Landesdatenschutzbehörde entschieden, unter welchen Bedingungen ein unverpixeltes Foto auf einer Facebook-Fanpage veröffentlicht werden darf (OVG Lüneburg, Beschl. v. 19.01.2021, 11 LA 16/20). Hintergrund des Verfahrens war die Veröffentlichung eines Fotos von einer Veranstaltung einer Partei, bei der es um den Bau einer Ampelanlage ging. Auf einem Foto, das insgesamt ca. 30 bis 40 Personen zeigt, die in einem Halbkreis um den Vorsitzenden des Ortsverbandes der Partei standen, waren auch die Eheleute F. abgebildet. Nachdem ca. vier Jahre später mit dem Bau der Ampelanlage begonnen wurde, stellte die Partei das anlässlich der Veranstaltung aufgenommene Foto für ihre Facebook-Fanpage ein. Die Gesichter der Eheleute F. waren auf dem Foto nicht verpixelt und das Foto war frei für sämtliche Facebook-Nutzer einsehbar. Die Eheleute F. beschwerten sich daraufhin bei der Landesdatenschutzaufsicht, die dem Ortsverband der Partei eine datenschutzrechtliche Verwarnung (Art. 58 Abs. 2 lit. a) DSGVO) erteilte. Dagegen hat die Partei letztlich erfolglos geklagt. Das OVG Lüneburg hat in zweiter Instanz das vorhergehende Urteil des VG Hannover bestätigt.

Die Veröffentlichung des unverpixelten Fotos ist nach der Entscheidung des OVG Lüneburg nicht gemäß Art. 6 Abs. 1 lit. f) DSGVO gerechtfertigt, da die Veröffentlichung eines unverpixelten Fotos für das berechtigte Interesse, über die parteipolitischen Aktivitäten zu informieren, nicht erforderlich war und das Ziel der Datenverarbeitung auch durch eine anonymisierte Verarbeitung hätte erreicht werden können. Im konkreten Fall ging es der Partei nicht darum, dass gerade die Eheleute F. als solche in einen spezifischen Kontext zur politischen Tätigkeit des Klägers gesetzt würden, sondern um den Nachweis, dass man sich politisch eingesetzt habe. In dem Fall hätten die Gesichter verpixelt werden müssen, was nach Auffassung sowohl des Verwaltungsgerichts als auch des OVG Lüneburg schon mit einfachen technischen Mitteln möglich gewesen wäre.

Die gemäß Art. 6 Abs. 1 lit. f) DSGVO durchzuführende Interessenabwägung fällt zugunsten der Eheleute F. aus. Das OVG argumentiert, dass den betroffenen Interessen ein hohes Gewicht zukomme, da die Daten im Internet veröffentlicht worden seien und somit ein Verlust der Kontrolle über die Daten drohe. Außerdem hätten die Eheleute F. vernünftigerweise nicht damit rechnen müssen, dass dieses Foto mehr als vier Jahre nach der Veranstaltung auf der Fanpage der Partei bei Facebook veröffentlicht würde. Allein die schlichte Tatsache, dass die Eheleute F. an der Veranstaltung teilgenommen hätten, begründe noch keine Beziehung zu der Partei, die die Veröffentlichung des Fotos mehr als vier Jahre nach der Veranstaltung auf der Fanpage vorhersehbar mache. Hinzu kommt, dass das Foto ohne Kenntnis der Eheleute F. aufgenommen worden sei und die Eheleute F. daher bereits zum Zeitpunkt der Datenerhebung keine Kontrolle über diese Daten gehabt hätten.

Die Veröffentlichung des Fotos auf der Facebook-Fanpage sei auch nicht gemäß §§ 22, 23 KUG gerechtfertigt. Die Normen seien bereits nicht gemäß Art. 85 Abs. 2 DSGVO anwendbar, da Art. 85 Abs. 2 DSGVO kein allgemeines Meinungsprivileg enthalte und somit nicht auf alle Meinungsäußerungen im Internet anwendbar sei. Insoweit beruft sich das OVG auch auf den Erwägungsgrund 153 zur DSGVO, wonach nur solche Tätigkeiten umfasst seien, die ausschließlich zu journalistischen Zwecken erfolgten. Die Veröffentlichung des Fotos auf der Facebook-Fanpage der Partei habe jedenfalls nicht ausschließlich journalistischen Zwecken gedient. Stattdessen habe die Partei auf ihre politischen Aktivitäten aufmerksam machen wollen. Die meinungsbildenden Zwecke haben jedenfalls nicht im Vordergrund gestanden.

Johanna Schmale

Datenschutzrechtliche Verantwortlichkeit bei der Nutzung von Instagram

Mehr als eine Milliarde Instagram-Konten weltweit werden nach Angaben von Facebook, dem Anbieter des sozialen Netzwerks, jeden Monat aktiv genutzt. Angesichts dieser Verbreitung verwundert es nicht, dass immer mehr Unternehmen Instagram für die Darstellung ihrer Produkte und zur Kundenansprache verwenden. Bei der Nutzung der verschiedenen Funktionen von Instagram, beispielsweise bei der Auswertung der Account-Nutzung über Instagram-Insights und der Schaltung von Werbung, wird eine Vielzahl an personenbezogenen Daten durch den Account-Inhaber, aber auch durch Facebook selbst, verarbeitet. Damit Unternehmen ihre datenschutzrechtlichen Pflichten bezüglich dieser Datenverarbeitung erkennen können, müssen sie sich zunächst die Frage stellen, inwieweit sie für die Datenverarbeitung verantwortlich sind. Dies geht aus den Nutzungsbedingungen und Datenrichtlinien von Facebook jedenfalls nicht ausdrücklich hervor.

Für den Betrieb einer Fanpage bei Facebook hat der Europäische Gerichtshof (EuGH) noch unter der Richtlinie 95/46/EG entschieden, dass der Fanpage-Betreiber gemeinsam mit Facebook für die Datenverarbeitung verantwortlich ist (EuGH, Urt. v. 05.06.2018, Az. C-210/16). Zur Begründung hat der EuGH u. a. ausgeführt, Fanpage-Betreiber würden durch das Einrichten der Fanpage einen aktiven Beitrag zu der Datenverarbeitung leisten und diese z. B. durch die Festlegung von Zielgruppen für Statistiken und Werbung maßgeblich beeinflussen. Hierdurch seien sie an der Entscheidung über die Zwecke und Mittel der Verarbeitung beteiligt.

Es stellt sich die Frage, ob diese Rechtsprechung zu den Facebook-Fanpages auf den Betrieb eines geschäftlichen Instagram-Accounts übertragbar ist. Nach den Nutzungsbedingungen und der Datenschutzrichtlinie von Instagram verwendet Facebook die über den Instagram-Account verarbeiteten Daten auch für eigene Zwecke, zum Beispiel für die Personalisierung der Plattform sowie für Werbezwecke. Die Tatsache, dass der Account-Inhaber auf diese Datenverarbeitung grundsätzlich keinen Einfluss hat, könnte in diesem Bereich für getrennte Verantwortlichkeiten sprechen. Allerdings werden die durch Facebook erstellten Auswertungen dem Account-Inhaber zu dessen Analysezwecken zur Verfügung gestellt. Er kann zudem über Targeting-Optionen Zielgruppen für die Anzeige von Werbung auswählen. Insofern kann eine Parallele zu den Facebook-Fanpages gezogen werden, indem zugrunde gelegt wird, dass auch bei Instagram der Account-Inhaber durch das Anlegen des Accounts den Anstoß für die Datenverarbeitung gibt sowie die weitere Datenverarbeitung durch Facebook beeinflusst. Es lässt sich also vertreten, zumindest in den Bereichen der Werbung und der statistischen Auswertungen, eine gemeinsame Verantwortlichkeit zwischen Facebook und dem Seitenbetreiber anzunehmen. In diesem Fall wäre mit Facebook eine Vereinbarung zur gemeinsamen Verantwortlichkeit nach Art. 26 DSGVO abzuschließen.

Das Datenschutzteam von BRANDI hat im September 2020 bezüglich der datenschutzrechtlichen Verantwortlichkeit bei der geschäftlichen Nutzung von Instagram eine Anfrage an den Datenschutzbeauftragten von Facebook gestellt. Facebook stellte in seiner Antwort fest, dass der EuGH die Annahme der gemeinsamen Verantwortlichkeit für Facebook-Fanpages wesentlich auf eine mittlerweile nicht mehr verfügbare Funktion stütze, die die Parametrierung zur Erreichung bestimmter Zielgruppen ermöglicht habe. Für die aktuelle Funktion in dem sozialen Netzwerk Facebook stelle die „Seiten-Insights-Ergänzung" von Facebook eine Vereinbarung zur gemeinsamen Verantwortlichkeit gem. Art. 26 Abs. 1 DSGVO dar. Instagram verfüge allerdings nicht über derartige Funktionalitäten, die der EuGH im Fall der Facebook-Fanpage für die Annahme einer gemeinsamen Verantwortlichkeit für ausschlaggebend gehalten habe. Instagram-Business-Profile würden deshalb weder von der Seiten-Insights-Ergänzung abgedeckt noch biete Facebook eine separate Vereinbarung für Instagram an.

Facebook sieht also für die geschäftliche Nutzung von Instagram keine gemeinsame Verantwortlichkeit mit dem Account-Betreiber. Hält man dennoch an einer gemeinsamen Verantwortlichkeit fest, was zumindest für die Bereiche der Werbung und der statistischen Auswertungen gut vertretbar ist, ergibt sich praktisch das Problem, dass darüber – anders als bei den Facebook-Fanpages – mit Facebook aktuell keine entsprechende Vereinbarung abgeschlossen werden kann. Die Darstellung einer gemeinsamen Verantwortlichkeit in der Datenschutzerklärung ohne Abschluss einer Vereinbarung nach Art. 26 DSGVO kann aber eine Datenschutzverletzung begründen. Dieses Risiko sollten Unternehmen insbesondere vor der Nutzung von Instagram-Werbung und Instagram-Insights berücksichtigen. Es bleibt abzuwarten, ob in der Zukunft eine höchstrichterliche Entscheidung – ähnlich wie zu den Facebook-Fanpages – zu der Klärung der Verantwortlichkeit beitragen kann. Bis dahin sollten Unternehmen bei der Darstellung der datenschutzrechtlichen Verantwortlichkeit für ihren Instagram-Account in ihrer Datenschutzerklärung abwägen, ob auf getrennte Verantwortlichkeiten oder – ohne den Abschluss einer entsprechenden Vereinbarung und daher mit dem erhöhten Risiko eines Datenschutzverstoßes – auf eine gemeinsame Verantwortlichkeit verwiesen werden sollte. Das Risiko einer Datenschutzverletzung lässt sich aktuell bei keiner der beiden Lösungsmöglichkeiten vollständig ausschließen; die zuerst genannte Alternative hat aber zumindest den Vorteil, dass im Verhältnis zu Facebook eine kohärente Darstellung vorliegt und nicht der Datenschutzverstoß aufgrund des Fehlens der Vereinbarung zur gemeinsamen Verantwortlichkeit begangen wird.

Dr. Sebastian Meyer, LL.M.

Datenschutzkonforme Nutzung von US-Diensten

Mit Einführung der Datenschutz-Grundverordnung (DSGVO) wurde ein einheitliches Datenschutzniveau innerhalb der Europäischen Union (EU) geschaffen, das den grenzüberschreitenden Datenaustausch in Europa deutlich vereinfacht hat. Gleichzeitig legt die DSGVO aber auch die Messlatte für den internationalen Datenaustausch sehr hoch. Jede Datenübermittlung in ein Drittland, also einen Staat außerhalb von EU und Europäischem Wirtschaftsraum (EWR), ist nur noch zulässig, wenn durch geeignete Maßnahmen ein vergleichbares Datenschutzniveau sichergestellt wird (Art. 44 DSGVO). Besondere Schwierigkeiten bereitet hierbei die Datenverarbeitung in den USA und – unabhängig vom Ort der Datenverarbeitung – die Zusammenarbeit mit amerikanischen Unternehmen. Ursprünglich hatten sich EU und USA auf das Safe-Harbor-Abkommen verständigt, was ein ausreichendes Datenschutzniveau auf amerikanischer Seite, vor allem durch eine freiwillige Selbstzertifizierung der teilnehmenden Unternehmen, erreichen sollte. Der EuGH hat jedoch die ausgehandelten Schutzmaßnahmen als nicht ausreichend angesehen und das Safe-Harbor-Abkommen für unwirksam erklärt (EuGH, Urt. v. 06.10.2015, Az. C-362/14). Das gleiche Schicksal ereilte die Nachfolgeregelung, das EU-US-Privacy Shield. Der EuGH hat vor allem Bedenken bezogen auf eine effektive Absicherung der Datenverarbeitung gegen Zugriffe durch staatliche Stellen in den USA (EuGH, Urt. v. 16.07.2020, Az. C-311/18 – Schrems II).

Formal bedeutet die Entscheidung des EuGH zunächst, dass alle Verträge mit amerikanischen Dienstleistern darauf geprüft werden müssen, ob diese noch Bezug nehmen auf das EU-US-Privacy-Shield. Diese Absicherung alleine reicht nicht mehr aus, so dass auf andere bzw. zusätzliche Maßnahmen ausgewichen werden muss. Der EuGH verweist darauf, dass auch bei amerikanischen Dienstleistern eine Absicherung nach den allgemeinen Grundsätzen durch die Nutzung von Standardvertragsklauseln als ein Baustein in Betracht kommen kann. Standardvertragsklauseln sind Musterbedingungen der Europäischen Kommission, die für gewisse Mindeststandards im internationalen Datentransfer sorgen sollen. Bestandteil der Standardvertragsklauseln ist unter anderem eine Regelung, wonach der Dienstleister garantieren soll, keinen Gesetzen zu unterliegen, die ihm die Einhaltung seiner Pflichten unmöglich macht, was durchaus fragwürdig ist. In diesem Kontext ist insbesondere zu beachten, dass die USA zuletzt massiv die Möglichkeiten des Zugriffs staatlicher Stellen auf gespeicherte Daten ausgeweitet haben. Der CLOUD Act (Clarifying Lawful Overseas Use of Data Act) aus 2018 sorgt etwa dafür, dass staatliche Stellen aus den USA selbst dann Zugriff auf Daten erhalten müssen, wenn diese außerhalb der USA

gespeichert sind (zum Beispiel auf Servern von Tochtergesellschaften in Europa). Die Aufsichtsbehörden akzeptieren daher bei amerikanischen Dienstleistern die Nutzung von Standardvertragsklauseln nur noch dann, wenn zusätzliche Sicherungsmaßnahmen ergriffen wurden und dokumentiert sind. In der Praxis gibt es in diesem Kontext aber erhebliche Unsicherheit, wie diese Anforderung konkret zu erfüllen ist. Auf europäischer Ebene hat der Europäische Datenschutzausschuss (EDSA) im November 2020 Empfehlungen veröffentlicht, aus denen sich einige Schutzmaßnahmen ableiten lassen (EDPB, Rec. 01/2020, adopted 10.11.2020). Besondere Bedeutung gewinnen dabei Maßnahmen zur Verschlüsselung und Pseudonymisierung, die einen unbefugten Zugriff auch durch staatliche Stellen einigermaßen effektiv verhindern können.

Zuletzt haben die Aufsichtsbehörden angekündigt, zukünftig auch im Rahmen von Stichprobenkontrollen überprüfen zu wollen, ob Unternehmen sich an die neuen Vorgaben halten. Politisch ist das Vorgehen durchaus umstritten, weil Unternehmen, die weiter amerikanische Dienstleister einsetzen wollen, gezwungen sind, alle Sachverhalte mit US-Bezug eigenständig zu prüfen und zu bewerten, nur weil auf politischer Ebene keine angemessene Absicherung der generellen Problematik erreicht werden konnte. Zwar arbeitet die Europäische Kommission aktuell an einer Überarbeitung ihrer Standardvertragsklauseln unter Berücksichtigung der letzten Entscheidungen des EuGH, die Aufsichtsbehörden akzeptieren es aber nicht, zunächst die Veröffentlichung der neuen Standardvertragsklauseln abzuwarten. Erschwerend kommt hinzu, dass es für viele Angebote großer amerikanischer Konzerne wie Google und Microsoft vielfach keine oder kaum angemessene europäische Alternativen gibt, auf die ersatzweise zurückgegriffen werden könnte.

In der aktuellen Situation führt daher kein Weg daran vorbei, zumindest vorläufige Maßnahmen zu treffen, um sich wegen des Einsatzes von amerikanischen Dienstleistern nicht angreifbar zu machen. Konkret bietet sich dabei ein gestuftes Vorgehen entsprechend der Empfehlungen des EDSA an.

1. Zunächst ist eine Analyse erforderlich, in welchen Bereichen überhaupt ein internationaler Datentransfer stattfindet. Zu erfassen ist nicht nur die Beauftragung von Dienstleistern mit Sitz in den USA, sondern auch europäischer Gesellschaften, die zu einem amerikanischen Konzern gehören; außerdem ist auch abzufragen, inwieweit Dienstleister ihrerseits Subunternehmer aus/in den USA einsetzen.

2. Für jede Datenverarbeitung mit US-Bezug ist sodann zu klären, auf welcher Grundlage diese erfolgt, also ob beispielsweise ein Rückgriff auf das unwirksame EU-US-Privacy Shield erfolgt oder die Geltung von Standardvertragsklauseln vereinbart wurde.

3. Basierend auf dem Umfang der Datenverarbeitung und der rechtlichen Absicherung hat eine Bewertung zu erfolgen, ob unter Berücksichtigung des Datenschutzniveaus im Drittland der Bedarf nach einer weiteren Absicherung besteht, was für die USA wohl immer anzunehmen sein wird.

4. Bei der zusätzlichen Absicherung sollte erst einmal in Erfahrung gebracht werden, welche Möglichkeiten der Dienstleister anbietet, da sich das Problem zumeist einheitlich oder ähnlich für alle europäischen Kunden auf Seiten des Dienstleisters stellen wird. Abgefragt werden sollten dabei insbesondere Möglichkeiten zur Verschlüsselung, wobei es wesentliche Unterschiede im Detail gibt.

5. Zusätzlich ist zu prüfen, ob neben den getroffenen Maßnahmen auch weitere formale Anforderungen bestehen, etwa die Information der Aufsichtsbehörde oder eine erforderliche Genehmigung.

6. Schließlich ist zu beachten, dass aktuelle Empfehlungen und Bewertungen regelmäßig überprüft werden müssen, insbesondere auch unter Berücksichtigung neuer Erkenntnisse oder geänderter rechtlicher Rahmenbedingungen.

Soweit für das Unternehmen ein eigener Datenschutzbeauftragter benannt ist, sollte das Vorgehen mit diesem abgestimmt und intern dokumentiert werden. Wichtig ist vor allem, dass für den Fall der Kontrolle ein Nachweis geführt werden kann, dass die Themen angegangen wurden.

Félix Paul

Datenschutz im Kartellrecht: Facebooks Nutzungsbedingungen

Die verschiedenen Aktivitäten von Facebook, oftmals als „Datenkrake“ bezeichnet, sind regelmäßig Gegenstand rechtlicher Diskussionen und gerichtlicher Entscheidungen in Deutschland. In den von Facebook verwendeten Nutzungsbedingungen ist zur Schaltung von Werbung – und damit zur Finanzierung des Unternehmens – die Verarbeitung und Verwendung von Nutzerdaten vorgesehen, die unabhängig von der Nutzung der Facebook-Plattform anfallen. Facebook bezieht sich dabei auf die Nutzung weiterer konzerneigener Dienste wie Instagram oder WhatsApp und die übergreifende Auswertung von Daten, etwa über Custom Audience oder bei der Nutzung des Buttons „Gefällt mir“. Facebook folgt einem einfachen Prinzip: Je mehr Daten Facebook zur Schaltung personalisierter Werbung zur Verfügung stehen, desto besser die Qualität der Werbung und desto mehr Profit kann das Unternehmen hieraus ziehen.

Nach dreijähriger Ermittlung untersagte das Bundeskartellamt (BKartA) mit Beschluss vom 6. Februar 2019 (Az. B6-22/16) Facebook die weitere Verwendung der Nutzungsbedingungen über die Zusammenführung der Daten, weil hierzu keine ausdrückliche und mithin keine datenschutzrechtlich hinreichende Einwilligung der privaten Nutzer eingeholt wurde. In den Nutzungsbedingungen von Facebook wird nämlich nur über Umwege in Form einer Verweisung auf eine Datenrichtlinie, die wiederum auf eine Facebook-Cookie-Richtlinie verweist, klar, dass eine solch intensive und umfassende Verwertung der personenbezogenen Daten stattfindet. Eben diesen wenig transparenten Nutzungsbedingungen müssen die Nutzer bei der Einrichtung des Facebook-Kontos zwingend zustimmen.

Im Rahmen des vorläufigen Rechtsschutzes hat der BGH auf die Rechtsbeschwerde des BKartA hin die Entscheidung des OLG Düsseldorf aufgehoben und den Antrag von Facebook auf Anordnung der aufschiebenden Wirkung der Beschwerde abgelehnt (BGH, Beschl. v. 23.06.2020, Az. KVR 69/19). Der BGH setzte ein

deutliches Zeichen, indem er feststellte, dass Facebook seine Marktmacht ausnutze, um auf diese Weise sehr weitgehende Rechte zur Datenverarbeitung gegenüber den Nutzern durchzusetzen. In seinem Beschluss setzte sich der Kartellsenat des BGH mit wesentlichen datenschutzrechtlichen Fragen im kartellrechtlichen Kontext auseinander. Dabei beurteilte der BGH, inwiefern die Nutzer der Plattform in ihrem Recht auf informationelle Selbstbestimmung aufgrund der mangelnden Wahlmöglichkeit betroffen sind. Der BGH stellt – für ein Eilverfahren – mit überraschender Klarheit fest, dass Facebook durch die Verwendung seiner bisherigen Nutzungsbedingungen, die nach der „Ganz-oder-gar-nicht-Mentalität" den Nutzern vorgelegt werden, diese missbräuchlich ausbeutet. Eben die fehlende „echte" Wahlmöglichkeit stellt aufgrund der sog. „Lock-in-Effekte", d. h. der hohen Wechselhürden für die Netzwerknutzer und der mangelnden Konkurrenz, eine kartellrechtlich relevante Ausbeutung der Nutzer dar, die sich auch nicht anhand der DSGVO rechtfertigen lässt.

Zusammenfassend lässt sich festhalten, dass Facebook seine marktbeherrschende Stellung durch die Verwendung seiner Nutzungsbedingungen missbraucht, wenn es von seinen Nutzern eine sehr umfassende Freigabe der eigenen Daten zur Nutzung durch Facebook als verpflichtende Voraussetzung für die Registrierung und Nutzung seiner eigenen Dienste verlangt.

Im Lichte dieser Entscheidung sollten Unternehmen bei der Konzeption ihrer Nutzungsbedingungen ausreichend hinterfragen, ob die dem Nutzer unterbreiteten Bedingungen auch tatsächlich hinreichend transparent und fair gestaltet sind.

Félix Paul
Wissenschaftlicher Mitarbeiter
felix-paul@brandi.net

Christina Prowald

Datenschutz und Homeoffice

In Anbetracht der Corona-Pandemie und nicht zuletzt der Verpflichtung von Arbeitgebern, ihren Mitarbeitern das Arbeiten auch in der eigenen Wohnung zu ermöglichen, hat die Relevanz des Themas Homeoffice im vergangenen Jahr deutlich zugenommen. Laut einer Umfrage des Forschungsinstituts zur Zukunft der Arbeit (IZA) im Auftrag des Bundesministeriums für Arbeit und Soziales arbeiteten annähernd die Hälfte der Beschäftigten Mitte Februar 2021 zumindest teilweise im Homeoffice (IZA Research Report No. 108).

In Deutschland müssen Unternehmen die datenschutzrechtlichen Vorgaben der DSGVO und des BDSG grundsätzlich auch dann einhalten, wenn Arbeitsleistungen außerhalb der betrieblichen Arbeitsstätte erbracht werden. Hierbei ergibt sich aus datenschutzrechtlicher Sicht typischerweise dadurch ein erhöhtes Risiko, dass der Arbeitgeber im Falle einer Tätigkeit im Homeoffice nur begrenzten Einfluss darauf hat, ob seine Mitarbeiter tatsächlich in einer Umgebung tätig sind, in der die Vertraulichkeit und Integrität der verarbeiteten Daten gewahrt ist. Um ein ausreichend hohes Datenschutzniveau sicherzustellen, empfiehlt sich eine Regelung der technischen und rechtlichen Rahmenbedingungen sowie die Verpflichtung der Mitarbeiter zur Wahrung der Vertraulichkeit und des Datengeheimnisses. Denkbar ist vor allem der Abschluss einer entsprechenden Vereinbarung zwischen dem Unternehmen und seinen Mitarbeitern unter Einbeziehung der nachfolgenden Aspekte:

1. Technische Voraussetzungen
Die sicherste Variante der Auslagerung von Tätigkeiten in das Homeoffice ist die ausschließliche Nutzung von dienstlich bereitgestellten IT-Systemen. Idealerweise erfolgt dabei der Zugriff auf die Systeme des Unternehmens über einen geschützten VPN-Zugang nach entsprechender Authentifizierung. Regelungsbedürftig ist dabei insbesondere die Tatsache, dass die überlassenen Arbeitsmittel ausschließlich zu betrieblichen Zwecken genutzt werden dürfen und eine Änderung der Sicherheitseinstellungen untersagt ist. Diese Gestaltung hat den Vorteil, dass das Unternehmen strikte Sicherheitsstandards durchsetzen kann und eine größtmögliche Kontrolle über die genutzten IT-Systeme behält.

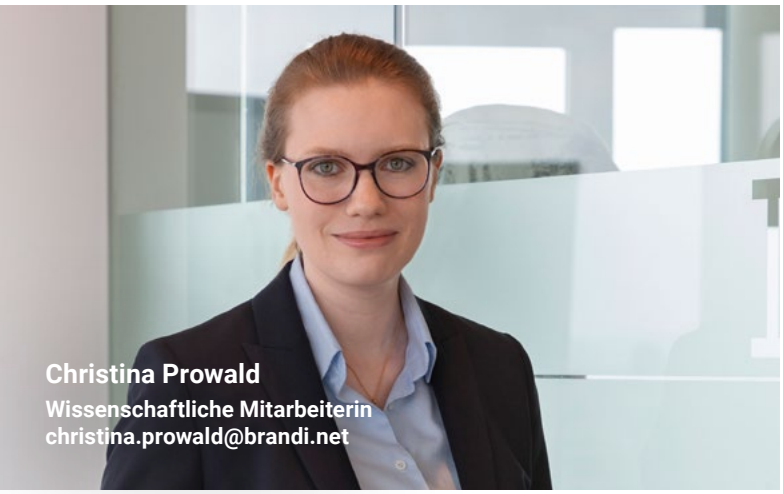
Grundsätzlich ist die Nutzung privater Geräte im Einzelfall ebenfalls denkbar. In Anbetracht der eingeschränkten Kontroll- und Zugriffsmöglichkeiten seitens des Arbeitgebers sowie der Problematik, dass dem Arbeitnehmer wohl kaum eine ausschließlich dienstliche Nutzung seines privaten Gerätes vorgeschrieben werden kann, ist Unternehmen jedoch von einem solchen Vorgehen im Regelfall aufgrund des erhöhten Risikos abzuraten. Ebenso sollte die Übertragung von Daten auf mobile Datenträger oder andere Speichermedien untersagt werden, da insoweit kaum zu kontrollieren ist, ob Dritte die Daten eingesehen haben und eine ordnungsgemäße Löschung erfolgt ist.

2. Datenschutzrechtliche Voraussetzungen
Darüber hinaus hat der Mitarbeiter dafür Sorge zu tragen, dass die überlassenen Arbeitsmittel sowie personen- und berufsbezogene Daten vor dem Zugriff durch Dritte geschützt sind und unberechtigte Personen keine Möglichkeit zur Kenntnisnahme von Daten des Unternehmens haben. Insbesondere sind die Daten vertraulich gegenüber Familienmitgliedern bzw. anderen Nutzern der Wohnung zu behandeln. Dies kann in der Regel nur dann gewährleistet werden, wenn die Geräte und Unterlagen in abschließbaren Bereichen aufbewahrt und die beruflichen Tätigkeiten nicht im Beisein anderer Personen ausgeübt werden.

Problematisch stellt sich vor allem die Ausübung der von der DSGVO vorgesehenen Kontrollpflichten des verantwortlichen Unternehmens dar. Zur ordnungsgemäßen Durchführung der Kontrollen muss aus Sicht der Aufsichtsbehörden „die Möglichkeit des Zugangs zur Wohnung des Beschäftigten" bestehen (BfDI, Faltblatt „Telearbeit und Mobiles Arbeiten"). Insoweit besteht jedoch ein Spannungsverhältnis zu der nach Art. 13 GG garantier-

ten Unverletzlichkeit der Wohnung. Das notwendige Zutrittsrecht erfordert aufgrund der Bedeutung des Art. 13 GG dabei das ausdrückliche Einverständnis des Mitarbeiters unter Einbeziehung des Einverständnisses der mit ihm in häuslicher Gemeinschaft lebenden Personen. Aus diesem Grund sollte zumindest die theoretische Möglichkeit vereinbart werden, dass das Unternehmen die Tätigkeit im Homeoffice erforderlichenfalls vor Ort zu Kontrollzwecken überprüfen darf. Sinnvoll ist auch die Verpflichtung der Mitarbeiter, Verstöße und Verdachtsfälle umgehend an den Arbeitgeber zu melden, damit gegebenenfalls erforderliche Maßnahmen zeitnah eingeleitet werden können.

Selbstverständlich können die einzelnen Regelungen beliebig detailliert und unter Berücksichtigung der unternehmenseigenen Besonderheiten ausgestaltet werden. Auf diese Weise kann dem erhöhten datenschutzrechtlichen Risiko wirksam begegnet und ein Absinken des Datenschutzniveaus verhindert werden.



Christina Prowald
Wissenschaftliche Mitarbeiterin
christina.prowald@brandi.net

Rebecca Vakilzadeh

Kennzeichnung von Affiliate-Links

Ein im Internet zunehmend beliebter werdendes Geschäftsmodell ist das Affiliate-Marketing, bei dem Betreiber von Internetseiten, sog. Affiliates, dort Produktlinks setzen, um auf die Webseite eines bestimmten Händlers zu verweisen. Gelangt ein Nutzer über diesen Link auf die externe Seite und tätigt dort eine Bestellung, so erhält der Affiliate eine Provision.

Dadurch dass die Affiliate-Links der Förderung des Absatzes Dritter dienen und durch dieses Verhalten folglich Werbung zu Gunsten dieser Anbieter betrieben wird, sind in diesem Zusammenhang bestimmte Kennzeichnungsvorschriften zu beachten.

Hierfür gelten neben den Regelungen des Telemediengesetzes (TMG) ebenfalls das Gesetz gegen den unlauteren Wettbewerb (UWG). § 6 Abs. 1 Nr. 1 TMG legt fest, dass kommerzielle Kommunikation, unter die im Falle der Zahlung einer Provision bei erfolgreicher Transaktion auch die Link-Setzung fällt, klar als solche gekennzeichnet sein muss. Dies ist nach der Vorschrift des § 5a Abs. 6 UWG wiederum nur dann der Fall, wenn sich der kommerzielle Charakter nicht unmittelbar aus den Umständen der Veröffentlichung ergibt. Eine Werbekennzeichnung ist demnach vor allem erforderlich, wenn die Links in überwiegend redaktionellen Beiträgen platziert werden oder wenn der Affiliate neutral erscheinende Produktvergleiche anstellt. Der Hinweis muss dabei so deutlich erfolgen, dass aus Sicht der jeweils angesprochenen oder betroffenen Verbraucherkreise kein Zweifel am Vorliegen eines kommerziellen Zwecks besteht.

Die Direktorenkonferenz der Landesmedienanstalten hat insbesondere im Zusammenhang mit Influencer-Marketing einen Leitfaden für die Werbekennzeichnung bei Social-Media-Angeboten veröffentlicht. Nach dem noch aktuellen Stand von Januar 2020 könnte in unmittelbarer Nähe des Produktlinks ein Sternchen-Hinweis zusammen mit folgender weiterführender Erläuterung erfolgen: „Die mit * gekennzeichneten Links sind sog. Affiliate Links. Kommt über einen solchen Link ein Kauf zustande, werde ich mit einer Provision beteiligt. Für Dich entstehen dabei keine Mehrkosten. Wo, wann und wie Du ein Produkt kaufst, bleibt natürlich Dir überlassen." An diese Formulierung sind die Zivilgerichte im Falle der Überprüfung der lauterkeitsrechtlichen Zulässigkeit der Kennzeichnung von Affiliate-Marketing jedoch nicht gebunden, so dass diesbezügliche Rechtsprechung ggf. auch strenger oder großzügiger ausfallen kann.

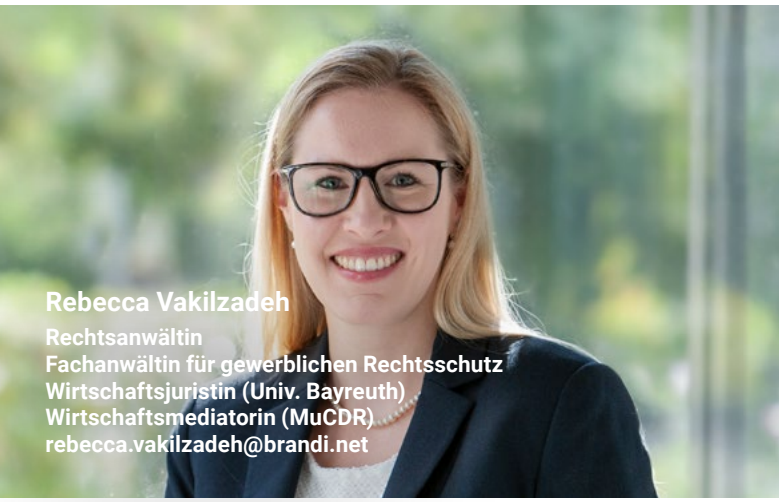
So ist gemäß einer Entscheidung des OLG Celle vom 8. Juni 2017 (13 U 53/17) die Verwendung des Hashtags „#ad" jedenfalls dann nicht ausreichend, um einen Beitrag als Werbung zu kennzeichnen, wenn er nicht deutlich und nicht auf den ersten Blick erkennbar ist. Im gegenständlichen Fall verwendete ein Influencer die genannte Kennzeichnung am Ende des Beitrags an zweiter Stelle von insgesamt sechs Hashtags. Nach Auffassung der zuständigen Richter ging die Kennzeichnung in der Vielzahl der gesetzten Hashtags unter. Ob und inwiefern der Hashtag „#ad" die notwendigen Kennzeichnungspflichten erfüllen würde, wenn er für die Verbraucher ohne jeden Zweifel erkennbar herausgestellt worden wäre, lässt das OLG Celle offen.

Nach Auffassung des LG Berlin (Urteil vom 11. Februar 2020 – 52 O 194/18) wurde die Bezeichnung „Shopping", die in kleiner Schrift über dem gegenständlichen Beitrag herausgestellt war, nicht als ausreichend zur Kennzeichnung eines Affiliate-Links angesehen. Das Gericht ging davon aus, dass es aus Sicht der angesprochenen Verkehrskreise um eine Rubrik mit der Bezeichnung „Shopping" gehen würde, also lediglich um die Angabe von Bezugsquellen für vorgestellte Produkte.

Erfolgt die Erläuterung des Produktlinks in Form eines Einkaufswagen-Symbols oberhalb der Überschrift des Beitrags in einem optisch abgetrennten Bereich, so ist dies ebenfalls lauterkeitsrechtlich unzulässig, urteilte das OLG Köln am 16. Dezember 2020 (6 W 102/20). Ein noch vor der Überschrift eingefügter Hinweis muss durch seine Aufmachung besonders hervorgehoben werden, um die Aufmerksamkeit des Lesers auf sich zu ziehen, und insbesondere so gestaltet sein, dass dem Leser der Bezug zum Beitrag verdeutlicht wird.

Ein besonders strenger Maßstab an die Erkennbarkeit des werblichen Charakters muss nach Auffassung des LG Hagen (Urteil vom 13. September 2017 – 23 O 30/17) dann gestellt werden, wenn mit dem jeweiligen Beitrag vor allem Kinder und Jugendliche angesprochen werden sollen. Die Vermischung von werbenden Elementen und solchen mit privatem Inhalt sei gerade für diese Zielgruppe nicht sofort erkennbar.

Zusammenfassend ist festzuhalten, dass jegliche Werbung für den Verbraucher klar, eindeutig und auf den ersten Blick erkennbar sein muss. Wann dies der Fall ist, kann stets nur durch Betrachtung sämtlicher Umstände des Einzelfalls beurteilt werden. Je mehr, vor allem höchstrichterliche Rechtsprechung, zu dem Thema vorliegt, desto konkreter werden sich die Anforderung an die werbliche Kennzeichnung eines Affiliate-Links bestimmen lassen.



Rebecca Vakilzadeh
Rechtsanwältin
Fachanwältin für gewerblichen Rechtsschutz
Wirtschaftsjuristin (Univ. Bayreuth)
Wirtschaftsmediatorin (MuCDR)
rebecca.vakilzadeh@brandi.net

Hendrik Verst

Die wettbewerbsrechtlichen Voraussetzungen an die werbliche Ansprache von Kunden

Viele Unternehmen wollen ihren unternehmerischen Erfolg mithilfe von Werbemaßnahmen verbessern, oder ihren Erfolg im Rahmen von Kundenzufriedenheitsbefragungen messen. Hierbei stellt sich in der Praxis die Frage, wann ein Kunde, beispielsweise nach dem Kauf einer Ware, nochmals angesprochen werden darf. Neben datenschutzrechtlichen Aspekten sind hierbei insbesondere wettbewerbsrechtliche Vorschriften zu beachten.

Die werbliche Ansprache von Kunden ist – ungeachtet etwaiger weitergehender inhaltlicher Anforderungen – im Gesetz gegen den unlauteren Wettbewerb (UWG) geregelt und ein Verstoß gegen die Vorschriften kann bei Beschwerden von Betroffenen oder Konkurrenten zu Abmahnungen und ggf. damit verbundenen Geldstrafen führen.

Als Werbung ist dabei jede Ansprache „mit dem Ziel der Absatzförderung" zu verstehen. Ausreichend ist dabei auch die mittelbare Absatzförderung. Der Begriff der Werbung ist damit denkbar weit und erfasst auch solche Kommunikation mit Kunden, die nicht unmittelbar auf den Verkauf von Produkten abzielt. In diese Kategorie fallen beispielsweise auch Kundenzufriedenheitsbefragungen im Nachgang zu einem erfolgten Kauf.

Gemäß § 7 Abs. 1 UWG darf durch die Werbung keine unzumutbare Belästigung entstehen. Damit so eine Belästigung nicht eintritt, muss die werbliche Ansprache bestimmte Voraussetzungen erfüllen.

Nach § 7 Abs. 2 Nr. 4 UWG muss die werbliche Nachricht einen Absender erkennen lassen und eine gültige Adresse enthalten, an welche der Adressat einen eventuellen Widerspruch richten kann. Weiterhin darf die werbliche Ansprache nicht gegen § 6 Abs. 1 des Telemediengesetzes verstoßen. Diese Vorschrift schreibt besondere Informationspflichten bei der kommerziellen Kommunikation vor. In diesem Rahmen ist auch für die Werbung ein Impressum erforderlich. Weiterhin muss die Werbung klar als solche erkennbar sein, so dass es zu keiner Verschleierung des Werbecharakters kommt. Bei Angeboten zur Verkaufsförderung sowie Gewinnspielen und Preisausschreiben müssen die Bedingungen für die Inanspruchnahme bzw. die Teilnahmebedingungen leicht zugänglich und unzweideutig angegeben werden.

Die weiteren Anforderungen sind abhängig von dem jeweiligen Medium, über welches geworben wird. Unterschieden wird hier im Wesentlichen zwischen postalischer und telefonischer Werbung sowie Werbung über ein anderes Fernkommunikationsmittel, typischerweise per E-Mail. Weiterhin ist oftmals zu differenzieren, ob gegenüber einem Verbraucher oder einem sonstigen Marktteilnehmer geworben wird. Der Begriff „Verbraucher" bezeichnet dabei eine natürliche Person, die ein Rechtsgeschäft zu Zwecken abschließt, die überwiegend weder ihrer gewerblichen noch ihrer selbstständigen beruflichen Tätigkeit zugerechnet werden können.

a) Postalische Werbung
Die postalische Werbung unterliegt den geringsten Anforderungen. Ist der Adressat Verbraucher, ist die Ansprache zulässig, sofern sie nicht hartnäckig erfolgt und nicht offensichtlich dem Willen des Betroffenen widerspricht. Sonstige Marktteilnehmer dürfen angeschrieben werden, außer es ist erkennbar, dass die Werbung nicht gewünscht ist. Die werbliche Ansprache per Post ist somit weitgehend unproblematisch. In der unternehmerischen Praxis sollte jedoch eine Sperrliste geführt werden, in welcher mögliche Widersprüche von Kunden erfasst werden und so gewährleistet ist, dass im Falle eines Widerspruchs keine weitere Ansprache des Betroffenen erfolgt.

b) Telefonische Werbung
Bei der telefonischen Werbung ist – wie bei der postalischen Werbung – zu unterscheiden, ob gegenüber einem Verbraucher oder einem sonstigen Marktteilnehmer geworben wird. Bei einem Verbraucher ist stets die ausdrückliche Einwilligung in die werbliche Ansprache erforderlich. Bei sonstigen Marktteilnehmern ist die mutmaßliche Einwilligung ausreichend. Für das Vorliegen einer mutmaßlichen Einwilligung muss das beworbene Produkt/die beworbene Dienstleistung zumindest objektiv dem Interesse des Betroffenen entsprechen. Hierfür ist es etwa ausreichend, dass der Betroffene ein vergleichbares Produkt gekauft hat.

c) Werbung per E-Mail
Erfolgt eine Werbung per E-Mail, ist stets die vorherige ausdrückliche Einwilligung des Adressaten erforderlich, unabhängig davon, ob es sich hierbei um einen Verbraucher handelt oder nicht.

Das Gesetz sieht in § 7 Abs. 3 UWG eine Ausnahme vom Erfordernis der Einwilligung bei der Ansprache per E-Mail vor. Eine werbliche Ansprache ist demnach auch möglich, wenn der Werbende die E-Mail-Adresse des Adressaten im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung erlangt hat, die Direktwerbung für eine ähnliche Ware oder Dienstleistung erfolgt, der Kunde der Verwendung nicht widersprochen hat und der Kunde bei der Erhebung der Adresse und bei jeder Ansprache

auf die jederzeitige Widerspruchsmöglichkeit hingewiesen wird. In diesem Rahmen kann beispielsweise nach einem Online-Kauf automatisch ein Newsletter versandt werden, soweit dieser sich auf vergleichbare Produkte bezieht und vorab auf die Zusendung von Werbung und die jederzeitige Widerspruchsmöglichkeit hingewiesen wird. Bei jeder Versendung des Newsletters sollte stets nochmals auf die jederzeitige Widerspruchsmöglichkeit hingewiesen werden.

Fazit:
Bei der werblichen Ansprache, die nicht den wettbewerbsrechtlichen Anforderungen genügt, drohen Unternehmen Abmahnrisiken durch Betroffene und Konkurrenten. Erfolgt die Werbung per Telefon oder E-Mail sollte somit bei Möglichkeit – auch zur Vermeidung von Rechtsunsicherheiten – stets die ausdrückliche Einwilligung der Betroffenen eingeholt und hinreichend dokumentiert werden. Werden die wettbewerbsrechtlichen Anforderungen an die werbliche Ansprache der Kunden eingehalten, lassen sich die werblichen Maßnahmen aus datenschutzrechtlicher Sicht, sofern nicht ohnehin die Einwilligung des Betroffenen nach Art. 6 Abs. 1 S. 1 lit. a) DSGVO eingeholt wird, jedenfalls auf die berechtigten Interessen nach Art. 6 Abs. 1 S. 1 lit. f) DSGVO stützen. Die datenschutzrechtliche Würdigung folgt im Rahmen der Interessenabwägung also der wettbewerbsrechtlichen Wertung.

Hendrik Verst
Wissenschaftlicher Mitarbeiter
hendrik.verst@brandi.net

Dr. Daniel Wittig

Verringerung des Abmahnrisikos im E-Commerce

Der E-Commerce wird für die Wirtschaft immer bedeutsamer. Dieser Trend bildete sich bereits vor der Corona-Krise deutlich heraus, beschleunigte sich aber wesentlich durch diese. Die Corona-Krise wirkte bei der Digitalisierung des Handels wie ein Katalysator, da während der einzelnen Lockdowns ein Online-Shop zeitweise der einzige Weg war, wie Händler ihre Waren ohne Einschränkungen weiter vertreiben konnten. Bisher ist ein Ende der Corona-Krise nicht absehbar. Es ist aber auch nach der Corona-Krise nicht davon auszugehen, dass sich der „Trend zur Digitalisierung" noch einmal umkehren wird. Umso bedeutsamer ist eine im Dezember 2020 erfolgte Gesetzesänderung im Gesetz gegen den unlauteren Wettbewerb (UWG), welche im Ergebnis das Abmahnrisiko im E-Commerce verringert.

Große Anzahl an Pflichten für Online-Shopbetreiber
Bei dem Betrieb eines Online-Shops gibt es zahlreiche Pflichten zu beachten. Auch das Internet ist kein rechtsfreier Raum. Insbesondere der E-Commerce ist durch Gesetze und Verordnungen, die vor allem die Verbraucher schützen sollen, stark reguliert. Dies betrifft sowohl die technische Ausgestaltung eines Online-Shops, als auch die Informationspflichten des Betreibers. Insbesondere die zahlreichen Informationspflichten stellen viele Shopbetreiber aber vor Probleme. So muss der Shopbetreiber beispielsweise über seine Identität, die technische Ausgestaltung des Shops, die Widerspruchsrechte des Verbrauchers, den Datenschutz, die Gesamt- und Grundpreise der einzelnen Produkte, die Sprachen des Vertragsschlusses, die Speicherdauer der Vertragstexte und vieles mehr informieren.

Hinzu kommt, dass sich die Angaben je nach Plattform, auf welcher man einen Shop betreibt, unterscheiden können. So müssen die Shopbetreiber auf der Plattform von Amazon andere Informationen bereithalten, als auf der Plattform von eBay.

Gefahr fehlender oder falscher Informationen
Erfüllt der Shopbetreiber die einzelnen Informationspflichten nicht, oder nicht richtig, so kann dies zum einen dazu führen, dass einem Kunden Rechte hieraus erwachsen. So können dem Kunden z. B. Schadensersatzansprüche zustehen, oder auch ein um ein Jahr verlängertes Widerrufsrecht. Zum anderen können aber auch Verbänden oder Mitbewerbern Ansprüche gegen den Shopbetreiber erwachsen. Dies ist der Fall, da eine fehlende oder fehlerhafte Information oftmals auch gleichzeitig als unlautere Handlung im Wettbewerb zu qualifizieren ist. Diese unlautere Handlung wiederum können Mitbewerber kostenpflichtig abmahnen. Zudem können die Mitbewerber von dem Shopbetreiber die Abgabe einer sogenannten strafbewehrten Unterlassungs- und Verpflichtungserklärung sowie den Ausgleich etwaig entstandener Schäden verlangen. Im Rahmen der strafbewehrten Unterlassungs- und Verpflichtungserklärung verpflichtet sich der Shopbetreiber gegenüber dem Abmahner, zukünftig den Wettbewerbsverstoß zu unterlassen und für den Fall eines erneuten Verstoßes, eine Vertragsstrafe an diesen zu zahlen.

Änderungen des UWG
Durch das Gesetz zur Stärkung des fairen Wettbewerbs wurden im Dezember 2020 jedoch einzelne Regelungen im UWG maßgeblich geändert. Ziel des Gesetzgebers war es, einen Missbrauch des Abmahnrechtes zu verhindern. Denn der Gesetzgeber registrierte besonders im E-Commerce eine hohe Missbrauchsquote von Abmahnungen. Durch die Gesetzesänderungen soll die „Abmahnindustrie", welche mit Wettbewerbsverstößen anderer Marktteilnehmer Geld verdient, eingedämmt werden. Insbesondere der Online-Handel war für die Entwicklung einer „Abmahnindustrie" prädestiniert, da es eine unübersichtliche Anzahl an Informationspflichten gibt und diese durch Computerprogramme, sogenannte Crawler, automatisiert überprüft werden können. Der vom Gesetzgeber festgestellten Entwicklung, dass einige Marktteilnehmer und Kanzleien für Massenabmahnungen von inhaltsgleichen Verstößen bekannt geworden sind und hiermit Geld verdienen, soll mit der Gesetzesänderung entgegengewirkt werden. Dies war unter der bisherigen Rechtslage nur unter eingeschränkten Voraussetzungen möglich. Ob das Ziel des Gesetzgebers tatsächlich erreicht wurde, soll aber im Rahmen dieses Artikels dahinstehen. In der Fachwelt ist dies bisher sehr umstritten.

Für Shopbetreiber können insbesondere zwei Punkte der Gesetzesänderung von großer Bedeutung sein. Zum einen müssen abgemahnte Shopbetreiber die Rechtsanwaltskosten des Abmahners im Falle einer Erstabmahnung nicht mehr zahlen, wenn der Informationspflichtverstoß im elektronischen Geschäftsverkehr oder in Telemedien, bzw. bezüglich Datenschutzinformationen geschieht und der Shopbetreiber in der Regel weniger als 250 Mitarbeiter beschäftigt. Zum anderen ist das Recht des Abmahners entfallen, im Zuge einer Abmahnung eine strafbewehrte, mithin mit einer Vertragsstrafe versetze, Unterlassungs- und Verpflichtungserklärung von dem abgemahnten Shopbetreiber zu fordern, wenn es sich um eine erstmalige Abmahnung bezüglich der Informationspflichten handelt und der Abgemahnte in der Regel weniger als 100 Mitarbeiter beschäftigt. Beides gilt für Abmahnungen von Wettbewerbern.

Durch die Einführung dieser Regelungen hat der Gesetzgeber gewissermaßen Verstöße gegen die Informationspflichten im elektronischen Geschäftsverkehr privilegiert und das Abmahnrisiko im E-Commerce verringert. Ob der Gesetzgeber alle seine Ziele mit der Gesetzesänderung tatsächlich erreicht, kann erst nach gewisser Zeit beurteilt werden. Fakt ist jedoch, dass sich insbesondere kleine und mittelständische Unternehmen nun besser gegen kostenpflichtige Abmahnungen wehren können und von diesen Abwehrmöglichkeiten auch Gebrauch machen sollten. Hierbei unterstützen wir sie gern.

Dr. Daniel Wittig
Rechtsanwalt
Datenschutzbeauftragter (TÜV ®) gemäß DSGVO und BDSG
daniel.wittig@brandi.net

Dr. Hans-Jürgen Buchmüller

Goldbären gegen Veggie-Bären

Wettbewerblicher Leistungsschutz für ein deutsches Kultprodukt
OLG Köln, Urt. V. 02.10.2020, Az: 6 U 19/20 = GRUR-RS 2020, 29679

Imagetransfer ist verlockend aber heikel. Das musste zuletzt der Hersteller veganer Gummibären, die Firma Vitana, erfahren, deren Gummibären von der Form her eine quasi-identische Nachahmung des Haribo-Goldbären waren und die zusätzlich in einer Verpackung vertrieben wurden, die der Verpackung der Goldbären ähnelte. Zunächst mit Einstweiliger Verfügung des LG Köln untersagt, bestätigte nun auch das OLG Köln im Berufungsverfahren der Hauptsache eine unlautere Nachahmung im Sinne des Wettbewerbsrechts und untersagte Vitana den Vertrieb ihrer Gummibären.

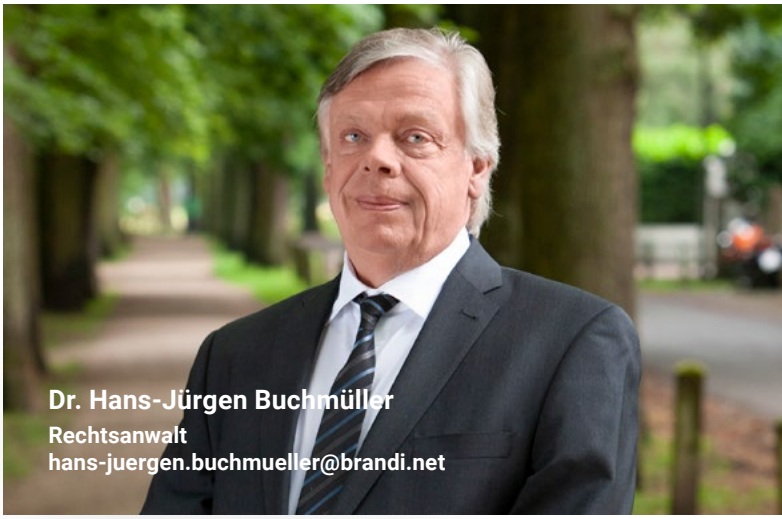
Was war konkret passiert? Die Firma Vitana hatte vegane Gummibärchen in den Geschmacksrichtungen Kirsche, Zitrone, Apfel, Orange, Erdbeere und Ananas in der Form der Goldbären auf den Markt gebracht. Diese vertrieb sie teurer als das Original, insbesondere über Reformhäuser, Biomärkte und das Internet. Auf der Verpackung war ein gelb-orangener Bär mit schwarzer Brille und grüner Fliege abgebildet, der ein Auge zukniff, die rote Zunge rausstreckte und bei nach vorn gestrecktem Arm den Daumen der linken Hand empfehlend hob. Gegen den Vertrieb der veganen Gummibärchen selbst wandte sich Haribo unter Berufung auf den lauterkeitsrechtlichen Nachahmungsschutz. Die Benutzung der Verpackung, wie beschrieben durch Vitana, wollte Haribo gestützt auf eingetragene Bildmarken untersagt sehen.

Das OLG Köln sah in den Gummibären der Firma Vitana eine unlautere Nachahmung im Sinne des § 4 Nr. 3b des Gesetzes gegen den unlauteren Wettbewerb, was den Unterlassungsanspruch zum Vertrieb der Bären für Haribo rechtfertigte. Die Benutzung der Vitana-Verpackung untersagte das OLG Köln nicht, weil es nicht feststellen konnte, dass diese mit der Verpackung der Goldbären verwechslungsfähig war.

Soweit das OLG Köln der Klage von Haribo stattgegeben hat, hat es sich auf die ständige Rechtsprechung des Bundesgerichtshofes zum wettbewerblichen Leistungsschutz gestützt. Danach kann der Vertrieb von Produktnachahmungen wettbewerbswidrig sein, wenn das nachgeahmte Produkt über wettbewerbliche Eigenart verfügt und besondere Umstände hinzutreten, die die Nachahmung unlauter erscheinen lassen. Als besondere Umstände gelten dabei die vermeidbare Täuschung über die betriebliche Herkunft des nachgeahmten Produkts oder eine unangemessene Beeinträchtigung oder Ausnutzung der Wertschätzung dieses Produkts. Dabei besteht eine Wechselwirkung zwischen dem Grad der wettbewerblichen Eigenart, der Art und Weise und der Intensität der Übernahme sowie den besonderen wettbewerblichen Umständen, so dass bei einer größeren wettbewerblichen Eigenart und einem höheren Grad der Übernahme geringere Anforderungen an die besonderen Umstände zu stellen sind, die die Wettbewerbswidrigkeit der Nachahmung begründen, und umgekehrt.

Das OLG Köln hat festgestellt, dass die Haribo-Goldbären wettbewerbliche Eigenart aufweisen. Wettbewerbliche Eigenart liegt vor, wenn die konkrete Ausgestaltung oder bestimme Merkmale eines Erzeugnisses geeignet sind, die angesprochenen Verkehrskreise auf seine betriebliche Herkunft oder seine Besonderheiten hinzuweisen. Die Goldbären hätten aufgrund ihrer charakteristischen Gestaltungsmerkmale, die sie von anderem Fruchtgummi in Bärenform unterscheidbar machen, jedenfalls eine durchschnittliche wettbewerbliche Eigenart, die dann aufgrund der jahrzehntelangen Marktpräsenz, des hohen Markterfolges und der durch Haribo getätigten erheblichen Werbeaufwendungen maßgeblich gesteigert sei. So seien sie geeignet, auf ihre betriebliche Herkunft hinzuweisen. Die wettbewerbliche Eigenart sei auch nicht durch eine mittlerweile auf den Markt gebrachte Vielzahl von Konkurrenzprodukten geschwächt, da sich der Goldbär nach wie vor von allen anderen Gummibärprodukten abhebe.

Unter Abwägung aller Umstände des Einzelfalls stellte das OLG Köln weiter fest, dass der Hersteller der Veggie-Bären die Wertschätzung der Verbraucher für die Goldbären für den Vertrieb seiner eigenen veganen Gummibären unangemessen ausnutzte. Es bestehe aufgrund der vielfältigen Gestaltungsmöglichkeiten für Fruchtgummi auch in Bärenform kein Zwang, die Goldbärenform zu verwenden. Wenn Vitana dennoch ohne Not und ohne berechtigtes Interesse eine quasi-identische Nachahmung geschaffen habe, spreche das mit Deutlichkeit dafür, dass dies geschehen sei, um sich an den guten Ruf der Goldbären anzulehnen. Die Verbraucher, denen die Goldbären seit vielen Jahren bekannt seien und die mit ihnen hohe Qualitätsvorstellungen verbinden würden, würden ihre Qualitätserwartung auf das Produkt der Firma Vitana übertragen, wodurch diese einen Imagetransfer erreiche, und ohne eigene Anstrengungen, z. B. durch Investitionen in die Bekanntheit ihrer Gummibären, unlauter am Markterfolg von Haribo partizipiere.



Dr. Hans-Jürgen Buchmüller
Rechtsanwalt
hans-juergen.buchmueller@brandi.net

Dr. Christoph Rempe

Umgestaltung und Vernichtung von urheberrechtlich geschützten Werken

Urheberrechtlich geschützte Werke können einem überall begegnen. Dies sind etwa Texte, Grafiken, Logos und Fotos, die Unternehmen für Werbematerialien in Auftrag geben. Urheberrechtlich können aber auch Gebrauchsgegenstände geschützt sein. Ebenso können Bauwerke und Kunstinstallationen urheberrechtlich geschützt sein. Dies führt schnell zu einem Spannungsverhältnis der Interessen desjenigen, der die Werke in Auftrag

gegeben hat, mit den Interessen des Urhebers. Daraus können sich Konflikte ergeben.

Die Unternehmen sollten sich daher darüber bewusst sein, dass sie nicht einfach Fotos, Texte, Grafiken oder Logos, aber auch Produkte, die ein Designer für das Unternehmen entworfen hat, ohne dessen Erlaubnis nutzen dürfen. Das Urheberrecht selbst kann nicht übertragen werden. Stattdessen können nach deutschem Recht lediglich Nutzungsrechte an einem Werk eingeräumt werden. Die Nutzungsrechtseinräumung sollte dringend vertraglich geregelt werden. Zwar gibt es Regelungen, wonach im Zweifel durch einen Arbeitnehmer in Erfüllung seiner Arbeitspflicht erschaffene Werke dem Unternehmen zustehen. Ansonsten gilt aber die sog. Zweckübertragungslehre, wonach der Auftraggeber eines Werkes im Zweifel immer nur diejenigen Nutzungsrechte von dem Urheber erhält, die für die vertraglich vorgesehene Verwendung erforderlich sind, aber nicht mehr. Auch hier setzt das Urheberrecht jedoch Grenzen, so wurde in der Rechtsprechung mehrfach entschieden, dass ein sog. „Rechte-Buy-out" jedenfalls in AGB-rechtlichen Regelungen unwirksam wäre, da dadurch der Urheber zu stark benachteiligt würde. Man sollte sich daher sehr nah am Zweck der Erstellung des Werkes orientieren. Jedenfalls sich die Nutzungsrechte einräumen lassen, die man sicher brauchen wird.

Dazu gehört auch das Bearbeitungs- sowie das Umgestaltungsrecht. Der Auftraggeber darf das Werk nämlich im Zweifel nicht einfach frei bearbeiten oder umgestalten. Die Bearbeitung ist vielmehr ebenfalls erlaubnispflichtig, sodass dies im Vertrag entsprechend geregelt werden sollte. Im Übrigen kann der Urheber, insbesondere von Kunstwerken oder besonderen Bauwerken, ggf. sogar deren Umgestaltung oder sogar den Abriss verbieten lassen. Insoweit tendiert der Bundesgerichtshof allerdings in der aktuellen Entscheidung dazu, dass die Interessen des Eigentümers an einer anderweitigen Nutzung oder Bebauung eines Grundstücks oder Gebäudes den Interessen des Urhebers am Erhalt des Werkes in der Regel vorgehen. Dies gilt auch für Kunstinstallationen in Gebäuden, weil sonst der Gebäudeeigentümer in seinen Eigentümerbefugnissen zu stark eingeschränkt wäre. In Streitfällen sind hier die gegensätzlichen Positionen miteinander abzuwägen.

Dr. Jörg König

Clickbaiting

Der BGH hat sich am 21.01.2021 (I ZR 120/19) mit der sog. Aufmerksamkeitswerbung befasst und seine diesbezügliche Rechtsprechung für die neuere Variante, das sog. Klickködern („Clickbaiting") im Internet, weiter entwickelt. Kläger war Günther Jauch, der schon vor einiger Zeit öffentlich erklärt hatte, er stehe für Werbung nicht mehr zur Verfügung. Er hat obsiegt.

Beim Clickbaiting werden besonders pointierte Meldungen oder Fotos eingesetzt, um die Neugier eines potenziellen Lesers zu wecken und diesen zu veranlassen, sich durch einen Klick auf die Nachricht oder das Foto dem verlinkten Beitrag zuzuwenden, wodurch Werbeeinnahmen mit den digital vorgehaltenen Medien erzielt werden. Wenn ohne Einwilligung Bilder (bekannter) Personen als Klickköder eingesetzt werden, stellt sich die Frage nach der Rechtmäßigkeit dieser Masche und den Ansprüchen, die der Betroffene aus einem etwa nicht gerechtfertigten Eingriff in sein Allgemeines Persönlichkeitsrecht herleiten kann.

Die Beklagte im Clickbaiting-Fall gibt u. a. die Programmzeitschrift „TV Movie" heraus und unterhält neben der Printausgabe die Internetseite www.tvmovie.de und ein Facebook-Profil. Darauf veröffentlichte sie am 18.08.2015 den Beitrag: „GERADE VERMELDET – Einer dieser TV-Moderatoren muss sich wegen KREBSERKRANKUNG zurückziehen. Wir wünschen, dass es ihm bald wieder gut geht", bebildert mit vier Fotografien, darunter Günther Jauch und der inzwischen verstorbene TV-Moderator Roger Willemsen. Die Meldung war mit der Internetseite verlinkt, auf der wahrheitsgemäß über die Krebserkrankung Roger Willemsens, nicht aber über Günther Jauch berichtet wurde. Günther Jauch verlangte Unterlassung und 20.000 Euro Schmerzensgeld, was ihm beides in allen Instanzen zugesprochen wurde. Ob ein Bild zu Werbezwecken, also kommerziell, eingesetzt wurde, sei, so der BGH, aus der Sicht eines Durchschnittslesers zu beurteilen. Ein Eingriff in den vermögensrechtlichen Zuweisungsgehalt des Rechts am eigenen Bild komme insbesondere dann in Betracht, wenn die Verwendung des Bildnisses den Werbe- und Imagewert des Abgebildeten ausnutze. Ausreichend sei, dass die Aufmerksamkeit des Betrachters auf das beworbene Produkt gelenkt werden solle. Eine Vereinnahmung des Abgebildeten für Werbezwecke könne nicht nur bei der Verwendung von Bildnissen in Werbeanzeigen, sondern auch bei einer redaktionellen Bildberichterstattung vorliegen, die (auch) der Eigenwerbung dient.

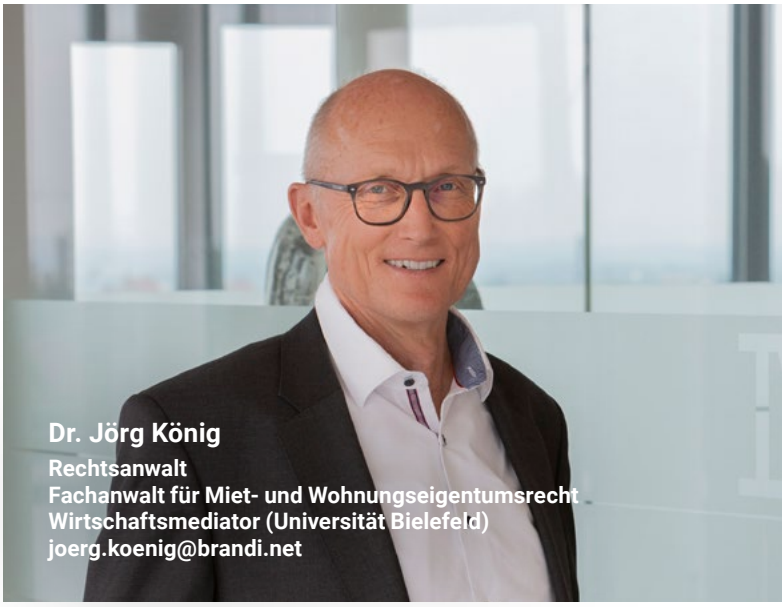
Die Verwendung des Fotos von Günther Jauch sei als kommerzielle werbliche Nutzung anzusehen. Die Beklagte habe damit Aufmerksamkeit für den verlinkten Zielartikel erregen wollen und diesen mit dem Posting pressetypisch beworben.

Die Nutzung des Bildes mit einer redaktionellen Berichterstattung ändere nichts am Einsatz zu Werbezwecken. Vielmehr sei Günther Jauch von der redaktionellen Berichterstattung in dem verlinkten Artikel nicht betroffen gewesen. Die bei der Beurteilung der Rechtmäßigkeit nach dem abgestuften Schutzkonzept gemäß den § 22, 23 KUG (im Kunsturhebergesetz geregeltes „Recht am eigenen Bild") vorzunehmende Interessenabwägung falle zu seinen Gunsten aus. Da er nicht eingewilligt habe, sei die Nutzung des Fotos nur zulässig, wenn das Bild dem Bereich der Zeitgeschichte oder einem der weiteren Ausnahmetatbestände zuzuordnen ist und berechtigte Interessen des Abgebildeten nicht verletzt werden. Der Begriff des Zeitgeschehens sei grundsätzlich nicht zu eng auszulegen. Es gehöre zum Kern der Pressefreiheit, dass die Presse innerhalb der gesetzlichen Grenzen einen ausreichenden Spielraum besitzt, in dem sie nach ihren publizistischen Kriterien entscheiden kann, was öffentliches Interesse beansprucht. Am Schutz der Pressefreiheit nimmt nach Art. 5 Abs. 1 Satz 2 GG auch die eigene Werbung für ein Presseerzeugnis teil, weil sie den Absatz des Presseerzeugnisses fördert und auf diese Weise zur Verbreitung der Informationen beiträgt. Auf eine Bildnutzung zur Berichterstattung über ein Ereignis des Zeitgeschehens könne sich jedoch nicht berufen, wer keinem schutzwürdigen Informationsinteresse der Allgemeinheit nachkomme, sondern durch Verwertung des Bildes eines anderen zu Werbezwecken allein sein Geschäftsinteresse befriedigen wolle. Der Verwendung des Bildes, komme, weil der Kläger weder Gegenstand der Berichterstattung in dem mit dem

„Clickbait“ verlinkten Artikel gewesen sei noch mit dem Gegenstand der Berichterstattung in Zusammenhang gestanden habe, kein Informationswert zu. Sie habe vielmehr nur Aufmerksamkeit auf den verlinkten Zielartikel erzeugen sollen.

Die Höhe der fiktiven Lizenzgebühr sei, wie bei Schadensersatzansprüchen, unter Berücksichtigung aller Umstände des Einzelfalles gemäß § 287 ZPO zu schätzen. Dabei sei dem überragenden Markt- und Werbewert des Klägers und seinem hohen Bekanntheitsgrad sowie dem Umstand Rechnung zu tragen, dass vernünftig handelnde Vertragspartner, auf deren Sichtweise abzustellen sei, bei der Verhandlung über eine angemessene Lizenzvergütung auch berücksichtigt hätten, dass das Bildnis im Zusammenhang mit einem sensiblen Thema (der Krebserkrankung eines TV-Moderators) werblich genutzt worden sei.

Damit hat der BGH einmal mehr die Grenzen einer ungefragten Nutzung eines Bildnisses aufgezeigt. Je geringer der Beitrag der Abbildung einer Person im konkreten Zusammenhang zur öffentlichen Meinungsbildung ist und je schwächer der inhaltliche Zusammenhang zwischen Bildnis und Berichterstattung oder der Werbung für letztere ausfällt, umso eher geht das Recht am eigenen Bild vor.



Dr. Jörg König
Rechtsanwalt
Fachanwalt für Miet- und Wohnungseigentumsrecht
Wirtschaftsmediator (Universität Bielefeld)
joerg.koenig@brandi.net

FRAGEN AN DR. LAURA SCHULTE

WARUM BRANDI?

Aus meiner persönlichen Perspektive machen vor allem zwei Aspekte BRANDI zu einem attraktiven Arbeitgeber. Zunächst verfügt BRANDI über eine ausgewiesene Expertise im Bereich des IT- und Datenschutzrechts und damit dem Rechtsgebiet, das mich spätestens seit meiner Zeit als wissenschaftliche Mitarbeiterin an der Universität Bielefeld am meisten fasziniert hat. Darüber hinaus verfügt BRANDI auch in diesem Rechtsgebiet über eine breit gefächerte Mandantschaft, vom innovativen Start-Up zum etablierten und weltweit agierenden Konzern. So werde ich über meine Arbeit als Rechtsanwältin in diesem Bereich täglich mit aktuellen und vielgestaltigen rechtlichen Herausforderungen im Bereich des IT- und Datenschutzrechts konfrontiert.

WAS TREIBT MICH AN?

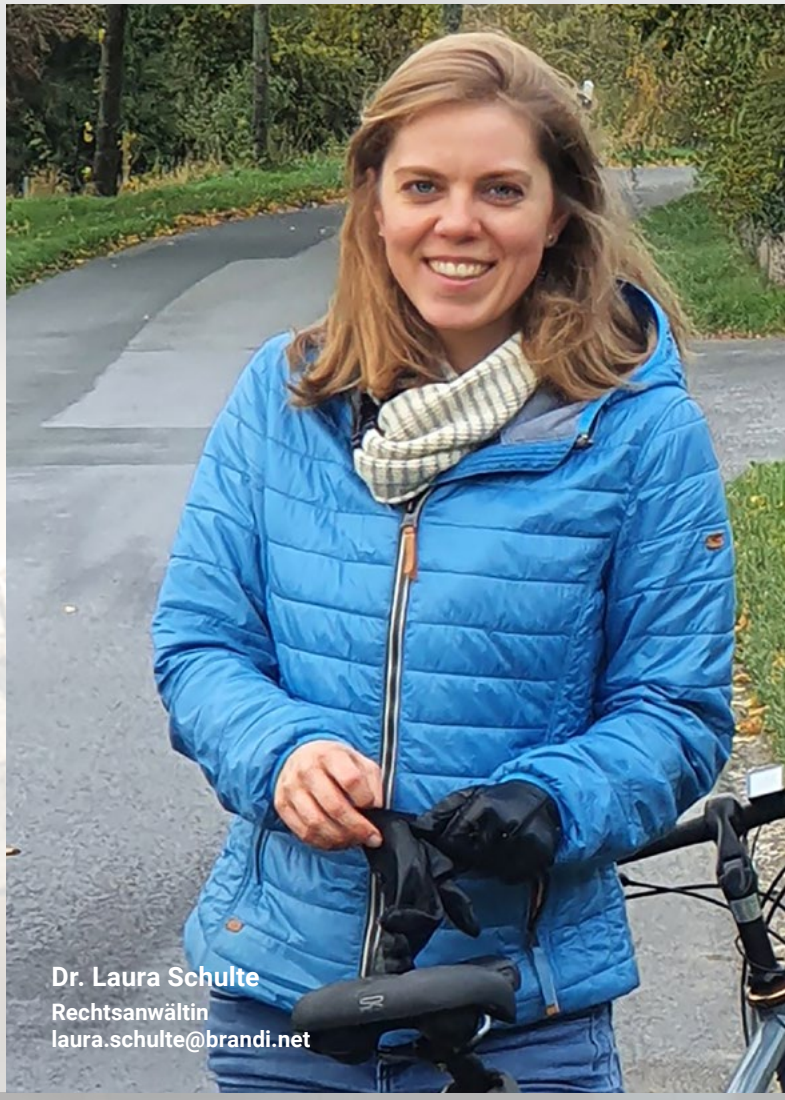
Das IT- und Datenschutzrecht ist ein noch verhältnismäßig junges Rechtsgebiet, das in weiten Teilen einem steten Wandel unterliegt und von höchster praktischer Relevanz ist. Die aktuelle Corona-Pandemie veranschaulicht deutlich, dass Informationstechnik sowohl im privaten, aber eben vor allem auch im unternehmerischen Bereich vielfach unverzichtbar geworden ist. Unsere Mandanten bei der Entwicklung von Lösungen in dem Spannungsfeld von neuen Rechtsentwicklungen, aktueller Rechtsprechung und aufsichtsbehördlicher Praxis sowie ihren praktischen Bedürfnissen zu unterstützen und mich dabei selbst stetig fortzuentwickeln, bildet meinen Antrieb.

AUSSER DEM JOB GIBT ES NOCH...?

... für mich vor allem meine Familie und Freunde, die bisweilen über meine Begeisterung für datenschutzrechtliche Fragestellungen verwundert sind. Außerdem gehört möglichst viel Bewegung zu meinem Alltag, kaum ein Wetter hält mich vom Fahrradfahren ab, ich jogge und wandere gerne im schönen Teutoburger Wald und mache Pilates. Es vergeht auch kaum ein Tag, an dem ich nicht noch zu einem – aus meiner Sicht – guten Buch greife.

HIGHLIGHTS AUS MEINER HEIMAT?

Da ich ganz Ostwestfalen zu meiner Heimat zähle, kann ich mit einigen Highlights aufwarten: Das Eggegebirge, an dem mein Heimatort Bad Driburg liegt, zählt sicherlich zu diesen. Daneben versuche ich mindestens einmal im Jahr das LWL-Freilichtmuseum in Detmold mit seinen wechselnden Ausstellungen zu besuchen. Eine Radtour von Schloß Neuhaus nach Paderborn an der Pader zählt außerdem zu meinen persönlichen Highlights. Schließlich verfügt meine Wahlheimat Bielefeld über zahlreiche schöne Orte, vom Siggi über das Bauernhaus Café an der Ochsenheide bis hin zum sog. Oetker-Park, um nur einige wenige zu nennen.



Dr. Laura Schulte
Rechtsanwältin
laura.schulte@brandi.net

Bielefeld
Adenauerplatz 1
33602 Bielefeld
T +49 521 96535 - 0
F +49 521 96535 - 99
E bielefeld@brandi.net

Detmold
Lindenweg 2
32756 Detmold
T +49 5231 9857 - 0
F +49 5231 9857 - 50
E detmold@brandi.net

Gütersloh
Thesings Allee 3
33332 Gütersloh
T +49 5241 5358 - 0
F +49 5241 5358 - 40
E guetersloh@brandi.net

Paderborn
Rathenaustraße 96
33102 Paderborn
T +49 5251 7735 - 0
F +49 5251 7735 - 99
E paderborn@brandi.net

Minden
Königswall 47-49
32423 Minden
T +49 571 83706 - 0
F +49 571 83706 - 66
E minden@brandi.net

Hannover
Adenauerallee 12
30175 Hannover
T +49 511 899379 - 0
F +49 511 899379 - 77
E hannover@brandi.net

Paris
44, Avenue des Champs Elyées
F-75008 PARIS
T +33 1 44 95 20 00
F +33 1 49 53 03 97
E info@kleinwenner.eu

Beijing
Grandall Law Firm
9th Floor Taikang Financial Tower
No. 38 North Road East Third Ring
Choayang
Beijing (Peking) 100026
T +86 10 65 89 06 99
F +86 10 58 13 77 88
E peking@brandi.net

www.brandi.net