HEUKING KÜHN LÜER WOJTEK

Newsletter
IP, Media & Technology

Januar 2015

RECHTSANWÄLTE UND STEUERBERATER

Inhaltsverzeichnis

Editorial

Informations- und Telekommunikationstechnik 2015 ff. – ab in die Wolken?!

Dr. Stephan Witteler
Rechtsanwalt
Standort: Frankfurt
s.witteler@heuking.de

Als eng mit der Informationstechnologie-Branche verbundene Rechtsanwälte verfolgen und begleiten wir täglich die Entwicklungen in diesem hochdynamischen Umfeld. Wo liegen die Trends? Welche „legal challenges 2.0" sind zu berücksichtigen?

Bekanntermaßen ist es immer wieder eine Herausforderung für Richter, Unternehmensjuristen und Anwälte, mit der technologischen Entwicklung Schritt zu halten. Der Prägung unseres Berufes folgend, haben wir dabei zumeist für die nötige rechtliche „Erdung" neuer IKT-Geschäftsmodelle Sorge zu tragen. Auch für uns stellt sich die Frage, wie man diesem Anspruch gerecht werden kann, wenn eine Branche explizit den Aufbruch in die „Wolken" deklariert.

Bekannte Schlagworte – neue Herausforderungen

Am Cloud Computing anknüpfend, entwickeln sich Standards, um den hiermit verbundenen Applikationen und/oder Rechenleistungen aus der „Steckdose" gerecht zu werden. Hiermit verbindet sich für uns auch ein erkennbarer Wechsel von hoch individualisierten Outsourcing- oder Computing-Services-Verträgen zu standardisierten Leistungen, die sich auf Grundlage ebenso standardisierter Vertragsmodelle umsetzen lassen. Während hierüber der Datenschutz vor vollkommen neue Herausforderungen gestellt wird, sehen Vertragsrechtler eine Entwicklung in Richtung „plain vanilla".

Ist damit IT-Vertragsrecht zur Massenware geworden? Auch wenn die Bewegung zur Cloud dies nahelegen könnte, stellen sich neue Herausforderungen in der zunehmend alle Geschäftsmodelle und Technikprojekte erfassenden IT-Standardisierung. Die Informationstechnologie ist heute bestimmender Faktor in nahezu allen technikaffinen Bereichen. Die Automatisierung in Logistik, Maschinenbau, Luftverkehr, Medizintechnik und Automobilbau schreitet rasant voran. Der IT-Jurist ist hier in hohem Maße gefordert. Sie/Er hat nicht nur das Know-how in Informations- und Kommunikationstechnologie zu entwickeln, sondern die spezifischen Geschäftsprozesse des jeweiligen Projektes in den diversen Branchen zu erfassen.

Informations- und Kommunikationstechnik bei Heuking Kühn Lüer Wojtek

Die IKT-Anwälte bei Heuking Kühn Lüer Wojtek haben sich dieser Entwicklung angenommen. Mit unserer Spezialisierung auf den öffentlichen Sektor, den Luftverkehrsbereich sowie die Logistik konnten wir in jüngster Zeit namhafte Großprojekte gewinnen. In diesem Sinne hat uns die besondere Anerkennung durch den JUVE Award für die IT-Kanzlei des Jahres 2014 sehr bestätigt. Selbstverständlich bleiben wir bei allen Projekten und auch Standardfragen – egal ob groß oder klein, komplexer oder einfacherer Natur – Ihr Ansprechpartner und freuen uns auf einen intensiven Dialog. In diesem Sinne hoffen wir, Ihnen mit der Themenauswahl dieses Newsletters eine interessante Grundlage zu vermitteln.

IPv6 und der Datenschutz

Dr. Lutz Martin Keppeler
Rechtsanwalt
Standort: Köln
l.keppeler@heuking.de

Die Einführung des IPv6-Standards ist in vollem Gange. Dies sollte in Unternehmen nicht nur die Systemadministratoren interessieren. Wenn die Vision Wirklichkeit wird, dass jedes Gerät im „Internet der Dinge" eine eindeutig zuordbare IP-Adresse erhält, wird dies auch juristische Konsequenzen haben. Gerade Unternehmen, die gegenwärtig erwägen, ihr Internetangebot IPv6-kompatibel zu gestalten, sollten vor allem die datenschutzrechtlichen Folgen im Blick haben.

Das Ende der alten IP-Adresse?

Der in den frühen 1980ern eingeführte IPv4-Standard ist an seine Grenzen gestoßen. Nachdem die Internet Assigned Numbers Authority (IANA) bereits 2011 symbolisch die letzten IPv4-Adressen an die kontinentalen Vergabestellen übergab, sind die rund 4,3 Milliarden herkömmlichen IP-Adressen vergeben, wenngleich auf lokaler Ebene derzeit noch ausreichend Adressen zur Verfügung stehen. Neue Adressen gibt es nicht, allenfalls werden nun durch Insolvenzen und freiwillige Rückgaben bereits belegte Adressen wieder frei.

Noch ist die IPv4-Adresse bei weitem die gebräuchlichste Form

Dennoch ist die herkömmliche IPv4-Adresse, bestehend aus vier Zahlen von 0 bis 255 (z. B. 157.134.2.57), derzeit noch die gebräuchlichste Form. Juristen haben sich an diese Adressform als Teil ihres Arbeitsalltags in der Strafverfolgung, bei der Durchsetzung zivilrechtlicher Ansprüche im Internet und im Datenschutzrecht gewöhnt. Wenn auch in Deutschland noch nicht alle Internetprovider auf IPv6 umgestellt haben (die Telekom bietet Neukunden seit September 2012 IPv6-Adressen an) und in einer langen Übergangszeit mittels des so genannten „Dual-Stack"-Verfahrens beide Formen der IP-Adressen gültig sein werden, ist es nun an der Zeit, sich über die rechtlichen Konsequenzen der Umstellung Gedanken zu machen.

Der neue Standard: IPv6

Die IPv6-Adresse besteht aus acht Viererblöcken und kann etwa so aussehen: „2001:0db8:85a3:08d3:1319:8a2e:0370:7347". Die 2^{128} möglichen Adressen reichen aus, um jedem Quadratmeter der Erdoberfläche über 600 Trilliarden Adressen zuzuweisen. Es ist also tatsächlich möglich, jedes technische Gerät über eine weltweit eindeutige Adresse anzusprechen. Dieses El Dorado

für Staatsanwälte und Cybercrime-Forensiker stellt sich für Datenschützer freilich als Sodom und Gomorrha dar.

Rechteverfolgung im Internet

Die Einführung von IPv6 hat bislang jedoch noch kaum zu neuen Identifizierungsmöglichkeiten von Rechteverletzern im Internet geführt, und dies ist auch vorerst nicht für die Zukunft zu erwarten. Vor allem liegt dies an der bislang geringen Verbreitung des neuen Standards. Auch wenn einige Provider bereits IPv6-Adressen vergeben, so liegt der gesamte Internet-Traffic, der über IPv6 abgewickelt wird, gegenwärtig noch bei unter einem Prozent. Wenngleich andere Indikatoren ein deutliches Ansteigen der Zahl der IPv6-Nutzer in diesem Jahr anzeigen (unter anderem gibt Google eine Statistik heraus, nach der Deutschland in der „IPv6-Adaption" im internationalen Vergleich besonders weit ist), werden vermutlich gerade die Webseiten-Betreiber und Filesharing-Netzwerke, welche zu Recht Abmahnungen befürchten, so lange bei IPv4 bleiben wie möglich. Der Betreiber eines Internetdienstes kann nämlich frei wählen, ob er IPv6-kompatibel sein will oder nicht.

Personenbezug durch IP-Adressen

Soweit sich Unternehmen für die Nutzung von IPv6 entscheiden, sollte diese Entscheidung datenschutzrechtlich begleitet werden, denn anhand einer IP-Adresse kann sich entscheiden, ob eine Information personenbezogen ist oder nicht. Nur wenn eine Angabe so konkret einer Person zugeordnet werden kann, dass ein personenbezogenes Datum vorliegt (§ 3 Abs. 1 BDSG) ist der Anwendungsbereich des Datenschutzrechts eröffnet. Vor allem bei einer dynamischen IPv4-Adresse – die bei jeder Einwahl neu an einen Nutzer vergeben wird – ist umstritten, ob diese hinreichend konkret auf eine bestimmbare natürliche Person hinweist. Während die Datenschutzaufsichtsbehörden überwiegend der Ansicht sind, dass jede dynamische IP-Adresse bereits ein personenbezogenes Datum darstellt, entschied das LG Berlin (Urteil vom 31.1.2013 - 57 S 87/08), dass nur unter bestimmten weiteren Voraussetzungen von einem hinreichenden Personenbezug auszugehen ist. Dieses Urteil wird allerdings gerade durch den BGH überprüft, der die delikate rechtliche Bewertung jüngst mit einer Vorlage an den EuGH übergeben hat (Beschluss vom 28.10.2014 - VI ZR 135/13). Die Klärung der längst überfälligen Frage wird möglicherweise nun in vielen Fällen bereits deshalb hinfällig, weil es möglich ist, eine weitaus größere Anzahl an statischen IPv6-Adressen zu vergeben.

Personenbezug trotz dynamischer IPv6-Adressen?

Doch auch im Rahmen von dynamischen Adressen dürfte IPv6 die Karten neu mischen. Es muss hier genauer als vorher zwischen dem Präfix der Adresse, die etwa einem Haushalt oder einer Firma zugeordnet wird, und dem Teil der Adresse, der einem Gerät zugeordnet werden kann, dem sog. „Interface-Identifier", unterschieden werden. Selbst wenn das Präfix dynamisch ist, kann dennoch möglicherweise anhand des „Interface-Identifier" eine eindeutige Zuordnung zu einem Gerät erfolgen, da für diesen Teil der IPv6-Adresse standardmäßig die sog. MAC-Adresse verwendet wird. Die MAC-Adresse identifiziert jedes mit dem Internet kommunizierende Gerät, wie Smartphones, moderne Fernseher, PCs, funkgesteuerte Rollläden oder Spielekonsolen, eindeutig. Es kann also sein, dass zwar niemand weiß, in welchem WLAN sich ein Laptop aufgehalten hat (da jedes WLAN über ein eigenes Präfix verfügt), aber dennoch aufgrund des Interface-Identifier etwa eine aufgerufene Website die IPv6-Adresse einem bestimmten Laptop exakt zuordnen kann.

Privacy Extensions: Nicht bei allen Betriebssystemen voreingestellt

Dagegen liefen freilich die Datenschutzaktivisten weltweit Sturm, mit der Folge, dass für die meisten gängigen Betriebssysteme sogenannte „Privacy Extensions" aktiviert werden können. Dadurch wird statt der MAC-Adresse ein zufällig generierter Interface Identifier verwendet. Doch vor allem die älteren Betriebssysteme verfügen nicht über diese Möglichkeit, und teilweise ist bei aktuellen Betriebssystemen die Funktion standardmäßig ausgeschaltet. Dies bedeutet: Wenn eine Webseite mit IPv6-Zugang angeboten wird, muss davon ausgegangen werden, dass viele ankommende IP-Adressen personenbezogene Daten sind, da es – anders als zuvor – je nach Einzelfall möglich ist, dass bei mehrfacher Anmeldung derselben MAC-Adresse auf ein Gerät und damit auf eine Person geschlossen werden kann. Dies ist jedenfalls die Ansicht der Aufsichtsbehörden. Da es allerdings für MAC-Adressen kein offizielles Register gibt, welches jedes einzelne Gerät erfasst, muss in jedem Einzelfall genau geprüft werden, ob es für die verantwortliche Stelle mit vertretbarem Aufwand möglich ist, die MAC-Adresse einer Person zuzuordnen. Der Hinweis der Aufsichtsbehörden, „zur Vermeidung datenschutzrechtlicher Probleme" (Orientierungshilfe Datenschutz bei IPv6, S. 12) stets von einem Personenbezug auszugehen, dürfte in vielen Fällen zu streng sein. Wie weit dies weitere Einwilligungserklärungen notwendig macht, kann nur im Einzelfall entschieden werden. Klar ist hingegen, dass die „Hinweise zum Datenschutz" auf der Webseite überarbeitet werden müssen, insbesondere wenn Trackingtools wie Google Analytics mit ih-

rer IPv6-Funktionalität genutzt werden. Inwieweit die bei IPv4 übliche „Kürzung“ der IP-Adresse auf IPv6 übertragen werden soll, ist derzeit noch nicht hinreichend geklärt.

Datenschutzaufsichtsbehörden beobachten IPv6

Jedenfalls aber ist klar, dass die deutschen Datenschutzbehörden das Thema IPv6 bereits frühzeitig auf die Agenda gestellt haben. Davon zeugt etwa die gemeinschaftlich verfasste „Orientierungshilfe Datenschutz bei IPv6“. Gerade die Tatsache, dass es bislang noch eher wenige IPv6-kompatible kommerzielle Webseiten gibt, könnte jedes Unternehmen, welches sich in diesen Bereich vorwagt, in den Fokus der Datenschutzaufsicht rücken lassen.

Fazit: Die Einführung von IPv6-Adressen wirft ein völlig neues Licht auf die Frage, ob anhand einer IP-Adresse ein Personenbezug hergestellt werden kann. Unternehmen, die ihren Internetauftritt IPv6-kompatibel gestalten, sollten diese Frage für sich beantworten, um nicht unnötig in das Fadenkreuz der Datenschutzbehörden zu geraten.

Open Source-Software in der Praxis

Dominik Eickemeier
Rechtsanwalt
Fachanwalt für
gewerblichen Rechtsschutz
Standort: Köln
d.eickemeier@heuking.de

Im Bereich Software unterscheidet man zwischen sogenannter proprietärer und Open Source-Software. Mit proprietärer Software ist diejenige Software gemeint, die Unternehmen entwickeln, um sie zum Beispiel an Dritte zu lizenzieren oder im eigenen Unternehmen zu verwenden. Ein wesentlicher Gesichtspunkt proprietärer Software ist derjenige der Verwertung. Unternehmen verdienen mit proprietärer Software Geld, indem sie sie verkaufen, sie lizenzieren oder Anwendungen betreiben – wie z. B. E-Shops im Rahmen des SaaS (= Software as a Service) –, für die ihre Kunden Geld bezahlen. Unter Open Source-Software verstehen viele freie, frei zugängliche und rechtsfreie Software. Dies ist nur teilweise richtig.

Die Open Source-Szene der freien Entwickler erarbeitet Software und ist dabei dem Gedanken verpflichtet, diese Software ohne Vergütung anderen zur Verfügung zu stellen. Diese anderen sollen die Software verwenden können und gegebenenfalls weiter entwickeln. Solche Software ist keineswegs urheberrechtsfrei, die Schöpfer dieser Software sind genauso wie diejenigen proprietärer Software Urheber im Sinne des Urheberrechts. Auch bei freier Software handelt es sich in der Regel um persönliche geistige Schöpfungen und damit um urheberrechtlich geschützte Werke. Die Schöpfer haben sich lediglich entschieden, die Software anderen kostenfrei zugänglich zu machen.

Copyleft

Im Gegenzug verlangen viele Open Source-Entwickler, dass derjenige, der ihre Software nutzt, ggf. erweitert oder verbessert, seine Arbeitsergebnisse wiederum allen Dritten ebenfalls kostenfrei zur Verfügung stellt. Dieses Prinzip des „Copyleft“ (eine etwas schiefe Verballhornung von „Copyright“) ist die wichtigste und prägnanteste Pflicht im Open Source-Bereich. Aber nicht alle Urheber von Open Source-Software erwarten diese Gegenleistung. Es kommt ganz darauf an, welche Lizenzbedingungen die jeweiligen Open Source-Entwickler ihrer Software zugrunde legen. Mit der Nutzung von Open Source-Software akzeptiert man stillschweigend die zugrunde gelegten Lizenzbedingungen. Es empfiehlt sich daher dringend zu ermitteln, welche Bedingungen bei der Nutzung der Software gelten sollen, und diese dann vorher sorgfältig zu lesen und zu prüfen.

Je nach der Art der Verbindung eigener Software mit Open Source-Software (z. B. Zusammenlegung in einer ausführbaren Datei) führt das „Copyleft"-Prinzip häufig zu dramatischen Ergebnissen. Unternehmen werden hierdurch gezwungen, Eigenentwicklungen im Quellcode preiszugeben, obwohl sie hierfür erhebliche Entwicklungskosten aufgewendet haben und diese Kosten sich durch eine entgeltliche Lizenzierung amortisieren sollten. Hierbei kommt es ganz entscheidend auf die Art der Verbindung der Softwarekomponenten an. Eine Planung im Vorhinein ist eminent wichtig, da häufig im Nachhinein die bereits gemachten Fehler nicht mehr behoben werden können.

Inkompatibilität von Open Source-Lizenzen

Werden Open Source-Softwarekomponenten unter verschiedenen Lizenzen miteinander kombiniert, können weitere Probleme auftreten. Hier ist insbesondere an die sogenannte Inkompatibilität solcher Lizenzen zu denken. Wenn sich Lizenzwerke nicht „miteinander vertragen", kommt es vor, dass bei der Verbindung solcher Softwarekomponenten unter den unterschiedlichen Lizenzen die Lizenzen als nicht erteilt gelten. Die Konsequenz wäre, dass der Verwender das Urheberrecht (der Open Source-Softwareentwickler) verletzt und auf Unterlassung und Schadensersatz in Anspruch genommen werden kann.

Software und Patente?

Für viele überraschend, können softwaretechnische Entwicklungen auch patentgeschützt sein. Etwa im Bereich der Umwandlung von Video- oder Audioformaten bestehen zahlreiche Patente. MP3 sei hier als Stichwort genannt. Viele der Patentinhaber haben sich zu Patent-Pools zusammengeschlossen, die Lizenzen an den Patenten vergeben. Ohne eine Lizenz liegen Patentverletzungen vor, die ebenfalls verfolgt werden können. Es drohen Unterlassungs- und Schadensersatzansprüche.

Fazit: Es empfiehlt sich daher unbedingt, bereits im Vorfeld eigener Softwareentwicklungen zu prüfen, ob überhaupt, und wenn ja in welcher Weise Open Source-Komponenten Verwendung finden sollen. Finden sie Verwendung, so ist eine genaue Dokumentation der verwendeten Komponenten, der betreffenden Lizenzen sowie der Art der Verbindung der einzelnen Komponenten ganz entscheidend.

Der (neue) Referentenentwurf für ein IT-Sicherheitsgesetz

Dr. Philip Kempermann, LL.M.
Rechtsanwalt
Standort: Düsseldorf
p.kempermann@heuking.de

Dr. Lutz Martin Keppeler
Rechtsanwalt
Standort: Köln
l.keppeler@heuking.de

Anfang November hat das Bundesministerium des Inneren einen neuen Referentenentwurf für ein IT-Sicherheitsgesetz veröffentlicht. Wenn auch der Erlass des Gesetzes nicht vor Mitte 2015 zu erwarten ist, lohnt sich aufgrund der vielfältigen Auswirkungen ein Blick auf den Entwurf. Die Änderungen betreffen unter anderem das BSI-Gesetz, das TMG und das TKG.

Auf einen noch relativ groben Referentenentwurf für ein IT-Sicherheitsgesetz vom 5. März 2013 des BMI folgten die Bundestagswahl, ein Koalitionsvertrag (der neun Mal den Begriff IT-Sicherheit verwendet und dem Begriff Cyberkriminalität einen eigenen Abschnitt widmet) und ein weiterer Referentenentwurf für ein IT-Sicherheitsgesetz am 18. August 2014, der am 4. November 2014 noch einmal aktualisiert und an europäische Entwicklungen angepasst wurde. Letzterer ist fast doppelt so lang wie sein Vorgänger, jedoch an entscheidenden Stellen immer noch so vage, dass für Unternehmen bedeutende Interpretationsspielräume entstehen. Dies gilt es zu nutzen.

Verpflichtung auf den „Stand der Technik" jetzt auch im TMG

TKG-Diensteanbieter mussten bisher schon das Fernmeldegeheimnis beachten und die Daten ihrer Nutzer dem Stand der Technik entsprechend schützen (§ 109 Abs. 1 TKG). Dass der Stand der Technik nun auch für die zusätzlichen Sicherheitspflichten eines Betreibers von öffentlichen Telekommunikationsnetzen gelten soll, ist noch kein großer Sprung. Dass aber nun auch Anbieter von gegen Entgelt angebotenen Telemedien auf Sicherheitsmaßnahmen verpflichtet werden, die den „Stand der Technik berücksichtigen müssen", dürfte einige Anbieter von Apps und Webseiten überraschen. Jedenfalls ist nun klar: Wer zu wenig für die Cybersicherheit seines Telemediendienstes unternimmt, sieht sich im Falle einer Datenpanne deutlich leichter einem Fahrlässigkeitsvorwurf ausgesetzt. Immerhin ist jeder noch so kleine kommerzielle App-Betreiber angewiesen, den Stand der Technik zu berücksichtigen. Was aber der Stand der Technik für Apps und Webseiten genau ist, mit dieser Gretchenfrage lässt der Gesetzgeber die Telemedienanbieter vorerst alleine. Doch bevor nun gerade kleinere TMG-Anbieter übereilt allzu große Investitionen in Sicherheitstechnik tätigen, lohnt ein Blick in die Begründung des Referentenentwurfs. Diesem lässt

sich nämlich entnehmen, dass Verhältnismäßigkeitsgesichtspunkte ebenfalls berücksichtigt werden können. Es muss also in jedem Einzelfall sorgfältig abgewogen werden, welche Sicherheitstechniken und welche organisatorischen Maßnahmen zum Einsatz kommen sollten.

Meldepflichten für Betreiber kritischer Infrastrukturen

Ein Kern des IT-Sicherheitsgesetzes besteht aus einer Meldepflicht für IT-Sicherheitsvorfälle, die sich bei Betreibern kritischer Infrastrukturen ereignen. Unternehmen müssen sich bewusst sein, dass für den Gesetzgeber nicht nur Atomkraftwerke und das Sicherheitsnetz der Deutschen Bahn als kritische Infrastruktur gelten. Es ist zwar vorgesehen, erst in einer Verordnung die kritischen Infrastrukturen näher zu definieren. Der Gesetzeswortlaut nennt aber bereits jetzt die folgenden Branchen: Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen. Anhand dieser Aufzählung darf bereits vermutet werden, dass der Begriff der kritischen Infrastruktur tendenziell eher weit verstanden wird.

Die Meldeflut

Nach dem neuen § 8b Abs. 4 BSI-Gesetz sollen die Betreiber kritischer Infrastrukturen „bedeutende Störungen" ihrer Systeme, die zu einem „Ausfall" oder einer „Beeinträchtigung" der betriebenen kritischen Infrastruktur führen „können", dem BSI melden. Die Meldepflicht soll also bereits ausgelöst werden, wenn eine Beeinträchtigung der IT zu einer potenziellen Beeinträchtigung der Infrastruktur führen kann. Das Potenzial zur Beeinträchtigung genügt folglich. Dies ist sehr weit, vor allem wenn man bedenkt, wie viele Cyberattacken täglich stattfinden. Die Deutsche Telekom sprach jüngst von gegenwärtig bis zu 450.000 Cyberangriffen pro Tag. Zwar wurde in dem jüngsten Entwurf der Begriff der „Beeinträchtigungen" der IT-Systeme durch das Tatbestandsmerkmal „bedeutende Störung" ersetzt, doch die Gesetzesbegründung verwässert diese scheinbar höhere Schwelle, indem sie darauf hinweist, dass auch bekannte Sicherheitslücken (die bei Standardsoftware regelmäßig gefunden werden) und nur versuchte Angriffe gemeldet werden sollen. Es ist daher nach wie vor unklar, ob es zum Beispiel in der Zukunft erforderlich wird, die Firewall-log-files auf „steckengebliebene" Angriffsversuche zu untersuchen und das Ergebnis an das BSI zu übersenden. Bedenkt man nun noch, dass die Meldung an das BSI Angaben zu den technischen Rahmenbedingungen, insbesondere der eingesetzten und betroffenen Informations-

technik enthalten muss, so fragt man sich, wie das BSI die ganzen Meldungen verarbeiten soll.

Aktuelle To-dos

Zur Beruhigung sollten sich Unternehmen an dieser Stelle Folgendes vergegenwärtigen: Erstens enthält die Definition der Meldepflicht eine Reihe ausfüllungsbedürftiger Begriffe, welche Unternehmen in ihrem Sinne interpretieren können. Zweitens enthält der Entwurf des IT-Sicherheitsgesetzes keine Sanktion für nicht gemeldete Beeinträchtigungen. Zudem sind anonyme und pseudonyme Meldungen vorgesehen. Andererseits werden Behörden ermächtigt, Anordnungen zur Beseitigung von Sicherheitsmängeln zu treffen. Daher gilt es jetzt bereits, bei größeren Unternehmen entsprechende Compliance-Richtlinien für den Umgang mit und die Dokumentation von „Beeinträchtigungen" vorzubereiten, um nicht später durch die Umsetzung des IT-Sicherheitsgesetzes überrascht zu werden.

Mehrere Meldeadressaten bei Diebstahl sensibler Daten

Besonders bunt wird es, wenn bei einem Infrastrukturbetreiber, etwa einer Bank oder einem Energieversorger, durch einen Cyberangriff auch sensible Kundendaten abhandenkommen. Dann muss neben einer Meldung an das BSI auch eine Meldung gemäß § 42a BDSG an die Datenschutzaufsichtsbehörden und die Betroffenen erfolgen. Bei börsennotierten Unternehmen ist gleichzeitig eine kapitalmarktrechtliche Ad-hoc-Meldepflicht zu prüfen. Es bleibt nur zu hoffen, dass durch den Erlass der so genannten NIS-Richtlinie auf europäischer Ebene nicht noch eine Meldestelle hinzukommt.

NIS-Richtlinie

Im Hintergrund zu den Debatten um den Entwurf des IT-Sicherheitsgesetzes ist zu bedenken, dass auf europäischer Ebene der Entwurf der Richtlinie zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union, der so genannten NIS-Richtlinie, voranschreitet. Der Kommissionsentwurf vom 7. Februar 2013 wurde in geänderter Fassung am 13. März 2014 durch das EU-Parlament angenommen. Diese weist in Teilbereichen einen deckungsgleichen Gegenstand mit dem IT-Sicherheitsgesetz auf. So werden auch hier Meldepflichten für Betreiber kritischer Infrastrukturen kodifiziert. Als Betreiber kritischer Infrastruktur waren im ersten Entwurf noch Betreiber von E-Commerce-Plattformen, sozialen Netzwerken, Cloud-Computing-Diensten und Application Stores genannt. Schon daran sieht man, wie wenig nationale und europäische Regulierungsbemühungen aufeinander abgestimmt sind. Der Anhang II des Richtlinienentwurfs, der die letztgenannten Bei-

spiele kritischer Infrastruktur auflistete, wurde in der vom Parlament angenommenen Version wieder gestrichen. Es wäre jedoch naiv anzunehmen, dass sich Europa nach dem deutschen IT-Sicherheitsgesetz richten wird. Vielmehr steht zu befürchten, dass die NIS-Richtlinie ein irgendwann 2015 erlassenes IT-Sicherheitsgesetz in vielen kleinen abweichenden Einzelfällen schnell wieder veralten lässt.

Fazit: Das IT-Sicherheitsgesetz lässt in seiner jetzigen Fassung viele Interpretationsspielräume offen. Was der Stand der Technik ist, wann eine Sicherheitsmaßnahme für einen Telemediendienstleister verhältnismäßig ist und wann eine bedeutende Störung der IT eine kritische Infrastruktur beeinträchtigen kann, wird auch bei Erlass des Gesetzes nicht klar sein. Eine Vielzahl von Fragen müssen nun in Unternehmen sorgsam abgewogen werden. Entsprechende Prozesse und Compliance-Richtlinien sollten umgesetzt sein, bevor das Gesetz in Kraft tritt.

Neue Auslegungshilfe zum „berechtigten Interesse“ des Datenverarbeiters

Dr. Lutz Martin Keppeler
Rechtsanwalt
Standort: Köln
l.keppeler@heuking.de

Im April diesen Jahres hat die Artikel 29-Datenschutzgruppe ein interessantes neues Papier herausgegeben: Mit der „Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/64/EC“ steht für die Rechtfertigung einer Datenerhebung/-verarbeitung auf Basis von „berechtigten Interessen“ eine neue Bibel des europäischen Datenschutzes zur Verfügung, die vor allem auch als Gegenentwurf zu den Äußerungen des Düsseldorfer Kreises über die Nutzung von personenbezogenen Daten für werbliche Zwecke gelesen werden kann.

Der Erlaubnistatbestand des berechtigten Interesses

Kernelement des Datenschutzrechtes ist das Verbot mit Erlaubnisvorbehalt. Für jede Erhebung, Verarbeitung und Nutzung (im Folgenden insgesamt „Verarbeitung“) von personenbezogenen Daten ist eine Erlaubnisnorm notwendig. Art. 7 lit. f der EU-Datenschutzrichtlinie (95/46/EG) zwingt sämtliche Mitgliedsstaaten dazu, die Verarbeitung von personenbezogenen Daten zu erlauben, wenn „berechtigte Interessen“ des Verarbeitenden gegeben sind und nicht von den Interessen der betroffenen Person überwogen werden. Im BDSG wurde dieses Prinzip schon vor Erlass der Richtlinie in § 28 Abs. 1 Nr. 2 kodifiziert. Aber wann liegt ein berechtigtes Interesse vor und wann überwiegt das stets vorhandene Interesse an der Geheimhaltung von Daten des Berechtigten?

Bislang europaweit uneinheitliche Handhabung

Aufgrund des großen Auslegungsspielraums des Begriffs „berechtigte Interessen“ wurde die entsprechende Erlaubnisnorm bislang in den Mitgliedsstaaten höchst unterschiedlich ausgelegt, auch wenn der EuGH gerade anhand von Art. 7 lit. f zuletzt erneut die Vollharmonisierung durch die EU-Datenschutzrichtlinie festgestellt hatte (EuGH, Urt. v. 24.11.2011, Rs. C-468/10 u. a.). Dieses Urteil und seine Vorgänger fanden in den Mitgliedsstaaten keine hinreichende Beachtung. Die deutsche Literatur will die Vorschrift relativ restriktiv anwenden. Bislang liegt nur wenig Rechtsprechung vor, die eine Datenverarbeitung aufgrund von § 28 Abs. 1 Nr. 2 BDSG gestattet. Bekanntestes Beispiel sind bislang Wirtschaftsauskunfteien, insbesondere die Schufa.

Der Begriff des berechtigten Interesses

Dies könnte sich nun ändern, denn die Art. 29-Datenschutzgruppe hat sich auf 68 Seiten allein mit der Interessenabwägung auf der Basis von Art. 7 lit. f der EU-Datenschutzrichtlinie beschäftigt

und klare Linien für die Abwägung vorgegeben. Die Anwendung dieser Abwägungsrichtlinien wurde zudem anhand von einigen Szenarien und 26 Beispielsfällen vorexerziert. Damit steht dem europäischen Datenschutzrecht ein einheitliches „Abwägungskompendium" bislang unbekannten Ausmaßes zur Verfügung.

Die Artikel 29-Datenschutzgruppe

Rechtsverbindlich ist die Opinion nicht im strengen Sinne. Um deren Bedeutung zu erfassen, muss man die Zusammensetzung und die Stellung der Artikel 29-Datenschutzgruppe näher betrachten. Namensgebend ist Art. 29 der EU-Datenschutzrichtlinie. Gemäß dieser Vorschrift entsendet jedes Mitgliedsland ein durch die nationale Datenschutzaufsicht bestimmtes Mitglied in die Gruppe, die ihre Beschlüsse mit einfacher Mehrheit fasst. Zusätzlich ist der Europäische Datenschutzbeauftragte stimmberechtigt. Für Deutschland ist die Bundesdatenschutzbeauftragte Angelika Vosshoff Mitglied der Gruppe. Die höchste deutsche Datenschützerin hat also Einfluss auf die Opinion nehmen können. Daher kann die Opinion in Deutschland bei den Datenschutzbehörden nicht ignoriert werden. Und das ist für Unternehmen positiv, da die Interessenabwägung in der Opinion durchaus liberaler gehandhabt wird, als dies bislang durch die deutschen Datenschutzbehörden der Fall war.

Liberale Interessenabwägung im Direktmarketing

Dies wird vor allem anhand der Beispiele im Direktmarketing deutlich: So wird etwa in einem Beispiel eine Werbe-E-Mail, die bestehende Kunden über Produkte informieren soll, aufgrund des „legitimen Interesses" des Shopbetreibers erlaubt, obwohl keine Einwilligung hierzu vorlag. Dabei spielt zwar auch eine Rolle, dass in dem konkreten Beispielsfall kein „komplexes Profil" des Kunden angelegt wurde und eine deutliche Opt-Out-Möglichkeit vorhanden war. Dennoch wird in rein datenschutzrechtlicher Hinsicht (auf europäischer Ebene wurde der strenge § 7 UWG nicht mitdiskutiert) der klare Widerspruch zu der bisherigen Linie der deutschen Datenschutzbehörden deutlich.

Strenge Regeln für das Direktmarketing durch den Düsseldorfer Kreis

Die strenge Auffassung des Düsseldorfer Kreises – des Zusammenschlusses aller deutschen Datenschutzbehörden – im Bereich des Direktmarketings zeigt sich in den „Anwendungshinweisen zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten für werbliche Zwecke" von Dezember 2013. Hier ziehen die Behörden teilweise überzogene Grenzen für die Anwendung von § 28 Abs. 3 BDSG, der Zentralnorm des Marketings im deutschen Datenschutzrecht. Zu dieser strengen Auslegung gehört auch die ebenfalls in der deutschen Literatur

bislang herrschende Ansicht, dass § 28 Abs. 3 BDSG eine Sperrwirkung gegenüber der allgemeinen Interessenabwägungsregel aus § 28 Abs. 1 Nr. 2 BDSG entfalte. Datenverarbeitungen zu Marketingzwecken sollen, so die Datenschutzaufsichtsbehörden, ausschließlich anhand von § 28 Abs. 3 BDSG entschieden werden.

Artikel 29-Gruppe erlaubt Lösung über allgemeine Abwägung bei Direktmarketingfällen

Ganz ausdrücklich spricht die Artikel 29-Gruppe an, dass ein paar Mitgliedsstaaten die allgemeine Interessenabwägungsregel falsch verstanden hätten. Diese sei nicht dazu da, nur in wenigen Ausnahmefällen die Lücke zu füllen, welche durch die Begrenztheit der anderen Erlaubnistatbestände entsteht. Vielmehr stehe der Erlaubnistatbestand des legitimen Interesses selbstständig neben den anderen Erlaubnistatbeständen. Eine Verdrängung des Anwendungsbereichs der berechtigten Interessen ergebe sich aus dem Text der EU-Datenschutzrichtlinie nicht.

Früherer oder späterer Abschied von § 28 Abs. 3 BDSG

Dazu passt gut, dass der gegenwärtige Entwurf der Datenschutzgrundverordnung keinen mit § 28 Abs. 3 BDSG vergleichbaren Erlaubnistatbestand aufweist. Vielmehr sind die Gründe für die Rechtmäßigkeit der Datenverarbeitung der alten Datenschutzrichtlinie nachempfunden. Art. 6 Nr. 1 lit. f des Entwurfes der Datenschutzgrundverordnung enthält den Rechtfertigungsgrund des „berechtigten Interesses“, welcher große Ähnlichkeit zu Art. 7 lit. f der Datenschutzrichtlinie aufweist. Es wird zukünftig daher ohnehin vermehrt auf ein „berechtigtes Interesse“ ankommen.

Beziehung zu § 7 UWG

§ 7 UWG wird weiterhin parallel zu den datenschutzrechtlichen Vorschriften zu prüfen sein. Der wettbewerbsrechtliche Aspekt des Direktmarketings wird durch die angesprochenen Entwicklungen nicht beeinflusst. Ob der Ansatz der Datenschutzbehörden, die Wertung aus § 7 UWG in die Abwägungen des Datenschutzrechts hineinzunehmen, nach der Opinion der Artikel 29-Gruppe und nach dem Erlass der Datenschutzgrundverordnung noch aufrechterhalten werden kann, bleibt abzuwarten.

Fazit: Die Opinion der Artikel 29 Gruppe verleiht dem datenschutzrechtlichen Erlaubnistatbestand des „berechtigten Interesses“ einen neuen Stellenwert. Dadurch können alte BDSG-Fragen an vielen Punkten neu bewertet werden. Insbesondere im Bereich des Direktmarketings ergeben sich durch die Opinion interessante Argumentationsmöglichkeiten gegen die deutschen Datenschutzaufsichtsbehörden.

BGH: Haftung für anonyme Bewertungen auf Internet-Bewertungsplattformen

BGH, Urteil vom 1.7.2014
(Az. VI ZR 345/13 – Ärztebewertungsportal)

Kai Runkel
Rechtsanwalt
Fachanwalt für gewerblichen Rechtsschutz
Standort: Köln
k.runkel@heuking.de

Leitsätze:

1. Dem durch persönlichkeitsrechtsverletzende Inhalte einer Internetseite (hier: zur Bewertung von Ärzten) Betroffenen kann ein Unterlassungsanspruch gegen den Diensteanbieter zustehen. Darüber hinaus darf der Diensteanbieter nach §§ 14 II, 15 V 4 TMG auf Anordnung der zuständigen Stellen im Einzelfall Auskunft über Bestands-, Nutzungs- und Abrechnungsdaten erteilen, soweit dies unter anderem für Zwecke der Strafverfolgung erforderlich ist.
2. Der Betreiber eines Internetportals ist in Ermangelung einer gesetzlichen Ermächtigungsgrundlage im Sinne des § 12 II TMG dagegen grundsätzlich nicht befugt, ohne Einwilligung des Nutzers dessen personenbezogene Daten zur Erfüllung eines Auskunftsanspruchs wegen einer Persönlichkeitsrechtsverletzung an den Betroffenen zu übermitteln.

Anmerkung: Der BGH hatte über die Rechtsfolgen einer unzulässigen, weil falsche Tatsachenbehauptungen enthaltenden, anonym abgegebenen Bewertung der fachlichen Leistungen eines Arztes auf einer hierfür vorgesehenen Internetplattform für den Plattformbetreiber zu entscheiden. Der betroffene Arzt hatte den ihn betreffenden, unrichtigen Blogeintrag gegenüber dem Plattformbetreiber beanstandet, der diesen daraufhin auch gelöscht hatte. Der anonyme Rezensent stellte seinen gelöschten Beitrag jedoch wieder ein. Dieses Spiel wiederholte sich offenbar, bis der Arzt schließlich den Plattformbetreiber auf Unterlassung und Auskunftserteilung über die Identität des Autors der unrichtigen Bewertung verklagte. Die Vorinstanzen gaben der Klage insgesamt statt; das Berufungsgericht ließ die Revision zu, allerdings beschränkt auf die Verurteilung zur Erteilung der Drittauskunft über den Verfasser der Bewertung. Der BGH hob die Verurteilung zur Auskunftserteilung auf.

Zwar geht der BGH davon aus, dass die allgemeinen Voraussetzungen eines Anspruchs gemäß § 242 BGB auf Erteilung einer Drittauskunft vorliegen. Jedoch dürfe der Plattformbetreiber eine solche Auskunft nicht erteilen, da § 12 Abs. 2 TMG dem entgegenstehe. Eine Rechtsvorschrift, die den Plattformbetreiber i.S.d. § 12 Abs. 2 TMG zur Weitergabe der Nutzerdaten des Verfassers der rechtswidrigen Bewertung ermächtigen würde, liege nicht vor. Die Vorschrift des § 242 BGB, aus der sich der akzessorische Auskunftsanspruch herleitet, beziehe sich nicht – wie von § 12 Abs. 2 TMG gefordert – ausdrücklich auf Telemedien. Die Vorschriften der §§ 14 Abs. 2, 15 Abs. 5 Satz 4 TMG kommen ebenfalls nicht als Ermächtigungsgrundlage in Betracht, da nach diesen Vorschriften eine Auskunftserteilung nur für die Zwecke der Strafverfolgung, der polizeilichen Gefahrenabwehr, der Aufgaben von Verfassungsschutz, BND, MAD und BKA sowie zur Durchsetzung der Rechte am geistigen Eigentum zulässig sei, nicht jedoch auch zum Zweck des Schutzes von Persönlichkeitsrechten. Eine analoge Anwendung der genannten Vorschriften scheide ebenfalls aus, da dem Gesetzgeber bei Schaffung des TMG ausweislich der Gesetzesmaterialien der Umstand, dass Persönlichkeitsrechtsverletzungen – anders als Verletzungen von geistigen Eigentumsrechten – nicht zur Auskunftserteilung gemäß §§ 14 Abs. 2, 15 Abs. 5 Satz 4 TMG ermächtigen, bewusst war und er gleichwohl auf eine diesbezügliche Regelung verzichtet hat, so dass es schon an der für eine analoge Anwendung der Vorschriften erforderlichen planwidrigen Regelungslücke fehle. Da dem Plattformbetreiber somit in Ermangelung einer gesetzlichen Ermächtigung zur Auskunftserteilung i. S. d. § 12 Abs. 2 TMG (bzw. – was natürlich auch ausreichend wäre, aber vorliegend ersichtlich ausschied – einer Einwilligung des betroffenen Nutzers in die Weitergabe seiner persönlichen Daten) die Auskunftserteilung rechtlich unmöglich sei (§ 275 Abs. 1 BGB), bestehe der mit der Klage geltend gemachte Auskunftsanspruch nicht.

Zu Recht weist der BGH in diesem Zusammenhang darauf hin, dass die Ungleichbehandlung der Auskunftserteilung bei Verletzung geistiger Eigentumsrechte einerseits und von Persönlichkeitsrechten andererseits wenig nachvollziehbar erscheint. Die Rechtsprechung kann an dieser Stelle aufgrund des klaren Gesetzeswortlauts und der bewussten Entscheidung des Gesetzgebers gegen eine Aufnahme der Persönlichkeitsrechte in den Ermächtigungskatalog der §§ 14 Abs. 2, 15 Abs. 5 Satz 4 TMG jedoch nicht weiterhelfen. Eine Änderung der Situation müsste der Gesetzgeber selbst herbeiführen.

Keine gesetzliche Ermächtigungsgrundlage zur Datenweitergabe

Unterlassungsanspruch gegen den Plattformbetreiber als Notlösung

Für den betroffenen Arzt ist hierdurch allerdings nicht alles verloren, denn ihm bleibt immerhin der Unterlassungsanspruch gegen den Plattformbetreiber (auch wenn er gegen den Verfasser der rechtswidrigen Bewertung selbst ohne Kenntnis von dessen Identität nicht vorgehen kann). Der Plattformbetreiber wird zumindest die weitgehend wortgleiche Wiedereinstellung der bereits gelöschten Bewertung (z. B. durch geeignete Software) verhindern können und müssen. Entsprechend der Rechtsprechung des BGH etwa zur Störerhaftung von File-Hosting-Dienstleistern für urheberrechtsverletzende Linksammlungen wird man ggf. auch eine manuelle Überprüfung jedenfalls der von dem betreffenden Nutzer eingestellten Inhalte auf kerngleiche Verstöße fordern können. Klar ist aber auch, dass dem betroffenen Arzt mit einem Vorgehen nur gegen den Plattformbetreiber weniger geholfen ist als mit einem Vorgehen gegen den Verfasser der falschen Bewertung selbst, denn nur hierdurch könnte schon der Einstellung weiterer rechtsverletzender Falschbehauptungen wirksam vorgebeugt werden.

Fazit: Persönlichkeitsrechtsverletzende anonyme Einträge in Telemediendiensten können de lege lata nur durch ein Vorgehen gegen den Plattformbetreiber und damit nicht mit optimaler Effizienz angegriffen werden. De lege ferenda müsste der Gesetzgeber aktiv werden, um an dieser Situation etwas zu ändern und eine gesetzliche Grundlage für die Weitergabe von Nutzerdaten durch den Plattformbetreiber an den von der Äußerung Betroffenen zu schaffen.

Leitsätze:

a) Der Geschäftsführer haftet für unlautere Wettbewerbshandlungen der von ihm vertretenen Gesellschaft nur dann persönlich, wenn er daran entweder durch positives Tun beteiligt war oder wenn er die Wettbewerbsverstöße aufgrund einer nach allgemeinen Grundsätzen des Deliktsrechts begründeten Garantenstellung hätte verhindern müssen.

b) Allein die Organstellung und die allgemeine Verantwortlichkeit für den Geschäftsbetrieb begründen keine Verpflichtung des Geschäftsführers gegenüber außenstehenden Dritten, Wettbewerbsverstöße der Gesellschaft zu verhindern.

c) Der Geschäftsführer haftet allerdings persönlich aufgrund einer eigenen wettbewerbsrechtlichen Verkehrspflicht, wenn er ein auf Rechtsverletzungen angelegtes Geschäftsmodell selbst ins Werk gesetzt hat.

Anmerkung: In dem dieser Entscheidung zugrunde liegenden Rechtsstreit ging es um irreführende Aussagen, die von selbstständigen Handelsvertretern bei der Haustürwerbung für Gaslieferverträge getätigt worden waren. Die betreffenden Handelsvertreter waren von einem Direktvertriebsunternehmen, welches seinerseits im Auftrag des Gasversorgers handelte, mit dem Vertrieb der Gaslieferungsverträge im Wege der Haustürwerbung beauftragt worden. Ein Wettbewerber nahm nicht nur das Direktvertriebsunternehmen, sondern auch dessen Geschäftsführer auf Unterlassung, Auskunft und Schadensersatz in Anspruch. Nachdem das Direktvertriebsunternehmen seine erstinstanzliche Verurteilung hingenommen hatte, hatte der BGH nur noch über die persönliche Haftung des Geschäftsführers zu entscheiden. Das Landgericht Berlin hatte den Geschäftsführer noch antragsgemäß verurteilt, da er Kenntnis von den Wettbewerbsverstößen gehabt und seinen Betrieb nicht so organisiert habe, dass er die Einhaltung von Rechtsvorschriften habe sicherstellen können. Das Kammergericht hatte auf die Berufung des Geschäftsführers das erstinstanzliche Urteil abgeändert und die Klage gegen diesen abgewiesen. Der BGH bestätigte diese Entscheidung.

BGH: Keine automatische Geschäftsführerhaftung für Wettbewerbsverstöße der Gesellschaft

BGH, Urteil vom 18.6.2014
(Az. I ZR 242/12 – Geschäftsführerhaftung)

Kai Runkel
Rechtsanwalt
Fachanwalt für
gewerblichen Rechtsschutz
Standort: Köln
k.runkel@heuking.de

Änderung der bisherigen Rechtsprechung

Allerdings entsprach es bislang der höchstrichterlichen Rechtsprechung, dass der Geschäftsführer persönlich für Wettbewerbsverstöße der Gesellschaft haftet, wenn er Kenntnis von ihnen hat und es unterlässt, sie zu verhindern. An dieser Rechtsprechung hält der BGH ausdrücklich nicht fest, da sie ihre Grundlage im Konzept der sog. Störerhaftung hat, die nach der neueren BGH-Rechtsprechung jedoch nur noch bei der Verletzung absoluter Schutzrechte wie Marken, Patente etc. gilt, nicht mehr jedoch bei Fällen von reinem Verhaltensunrecht wie etwa Wettbewerbsverstößen. Es ist daher konsequent, wenn der BGH sich nun auch von der lediglich kenntnisabhängigen Geschäftsführerhaftung kraft Organstellung verabschiedet.

Das bedeutet jedoch nicht, dass der Geschäftsführer bei wettbewerbswidrigem Verhalten seiner Gesellschaft überhaupt keine persönliche Haftung mehr zu befürchten hätte. Der BGH stellt vielmehr eine ganze Reihe von Fallkonstellationen dar, in denen eine solche persönliche Haftung nach wie vor anzunehmen ist, verneint deren Vorliegen aber jeweils für den konkret entschiedenen Fall.

Haftung des Geschäftsführers als Täter oder Teilnehmer der Wettbewerbsverletzung

So haftet der Geschäftsführer (natürlich) immer dann persönlich, wenn er an dem Wettbewerbsverstoß persönlich mitgewirkt, ihn unterstützt oder ihn in Auftrag gegeben hat (dann nämlich als Täter, Gehilfe oder Anstifter, jedenfalls wegen positiven Tuns). Ein Rückgriff auf die überkommenen Grundsätze der Störerhaftung ist in diesen Fällen von vornherein entbehrlich.

Interessant ist in diesem Zusammenhang die Aussage des BGH, ausreichend für eine Verurteilung des Geschäftsführers als Täter könne ein Verhalten sein, „das nach seinem äußeren Erscheinungsbild und mangels abweichender Feststellungen dem Geschäftsführer anzulasten ist", was etwa bei rechtsverletzender Benutzung einer bestimmten Firmierung oder „dem allgemeinen Werbeauftritt" des Unternehmens anzunehmen sei, weil über solche Fragen „typischerweise auf Geschäftsführungsebene entschieden" werde. Daraus folgt, dass der Geschäftsführer z. B. zur Haftung für irreführende Werbeaussagen auf der Website seines Unternehmens herangezogen werden kann, sofern nicht festgestellt werden kann, dass er über deren Gestaltung nicht mitentschieden hat. Der Sache nach handelt es sich insoweit um eine widerlegbare Vermutung, was zugleich bedeuten dürfte, dass der Geschäftsführer die Darlegungs- und Beweislast dafür trägt, die betreffende Maßnahme nicht veranlasst zu haben.

Haftung des Geschäftsführers aus Garantenstellung

Daneben kann der Geschäftsführer unter Umständen aber auch dafür haftbar gemacht werden, dass er eine wettbewerbswidrige Handlung der Gesellschaft nicht verhindert hat, also letztlich für ein Unterlassen. Voraussetzung hierfür ist jedoch eine gegenüber außenstehenden Dritten bestehende Rechtspflicht des Geschäftsführers zum Handeln, nämlich zur Verhinderung dieses Verhaltens. Aus der bloßen Organstellung als Geschäftsführer folgt eine solche Verpflichtung noch nicht; daraus lässt sich nur eine Verpflichtung des Geschäftsführers gegenüber der Gesellschaft ableiten, dafür zu sorgen, dass die Gesellschaft sich rechtskonform verhält, aber keine Verpflichtung gegenüber außenstehenden Dritten wie insbesondere den Wettbewerbern der Gesellschaft. Es bedarf vielmehr einer Erfolgsabwendungspflicht im Sinne einer Garantenstellung des Geschäftsführers gegenüber dem anspruchstellenden Wettbewerber nach den Regeln des allgemeinen Delikts- und Strafrechts. Eine solche kann aus vorangegangenem gefährdendem Tun (Ingerenz), aus Gesetz, Vertrag oder der Inanspruchnahme besonderen Vertrauens folgen. Von besonderer praktischer Bedeutung ist die Garantenstellung aus Ingerenz.

Insbesondere: Wettbewerbsrechtliche Verkehrspflichten zur Gefahrabwendung

Der BGH hat in jüngerer Zeit damit begonnen, in einer Reihe von Entscheidungen näher zu konkretisieren, in welchen Fällen insbesondere sog. wettbewerbsrechtliche Verkehrspflichten zur Abwendung der Gefahren bestehen, die aus der Schaffung oder Aufrechterhaltung einer wettbewerblichen „Gefahrenquelle" des Haftenden resultieren. Dieses Verkehrspflichtenmodell soll als Nachfolgemodell zur überholten Störerhaftung dienen. Soweit es die Haftung für ein Unterlassen betrifft, geht es hierbei der Sache nach um einen Fall von Ingerenz. Ein abschließend klares Bild, unter welchen Voraussetzungen wettbewerbsrechtliche Verkehrspflichten zur Gefahrabwendung bestehen, fehlt bislang. Der BGH fügt mit der vorliegenden Entscheidung allerdings einige Mosaiksteine hinzu: So stellt er etwa klar, dass aus der bloßen Aufnahme oder Ausübung von grundsätzlich wettbewerbsrechtlich zulässigen Aktivitäten (hier: Direktvertrieb von Gaslieferungsverträgen durch Haustürwerbung) noch keine wettbewerbsrechtlichen Verkehrspflichten des Geschäftsführers zur Gefahrenabwehr folgen. Zwar könne auch durch zulässige Geschäftsmodelle eine gesteigerte Gefahrenlage hinsichtlich der möglichen Verletzung wettbewerbsrechtlicher Vorschriften hervorgerufen werden; wettbewerbsrechtliche Verkehrspflichten zur Gefahrenabwehr obliegen dann aber grundsätzlich nur dem Unternehmen und nicht ohne weiteres auch dem Geschäftsführer.

Anders könne es dann zu beurteilen sein, wenn der Geschäftsführer sich (z. B. durch permanente Auslandsabwesenheit) bewusst der Möglichkeit entziehe, überhaupt Kenntnis von etwaigen Wettbewerbsverstößen in seinem Unternehmen oder bei beauftragten Drittunternehmen zu erlangen und dagegen vorgehen zu können. Dafür sei aber das bloße Outsourcing von Werbemaßnahmen auf einen Subunternehmer wie im vorliegenden Fall ungeachtet der damit verbundenen geringeren Kontrollmöglichkeiten des Geschäftsführers nicht ausreichend, denn Outsourcing stelle eine grundsätzlich wettbewerbsrechtlich unbedenkliche Unternehmensentscheidung dar, die nicht per se als Gefahrenquelle für Wettbewerbsverstöße angesehen werden könne. Anders könne der Fall allerdings dann liegen, wenn gerade solche Unternehmen als Subunternehmer beauftragt würden, bei denen aufgrund besonderer Umstände von vornherein mit Wettbewerbsverstößen zu rechnen sei. Auch komme eine persönliche Haftung des Geschäftsführers dann in Betracht, wenn es um Rechtsverletzungen gehe, auf die das von dem Geschäftsführer „ins Werk gesetzte" Geschäftsmodell des Unternehmens gerade angelegt sei; hierfür bestanden im entschiedenen Fall jedoch keine Anhaltspunkte.

Fazit: Nach aktueller Rechtsprechung des BGH haftet der Geschäftsführer nicht (mehr) automatisch, sobald er Kenntnis von Wettbewerbsverstößen der Gesellschaft hat und nichts dagegen unternimmt. Vielmehr ist stets zu prüfen, ob der Geschäftsführer selbst an der Wettbewerbsverletzung aktiv beteiligt war; ansonsten kommt seine persönliche Haftung nur in besonders gelagerten Fällen in Betracht. Allerdings spricht eine (widerlegbare) Vermutung für die persönliche Beteiligung des Geschäftsführers an bestimmten grundlegenden (u. a. Werbe-) Maßnahmen der Gesellschaft, die typischerweise auf Geschäftsführungsebene beschlossen werden; hierzu zählt neben der Wahl der Firmierung der Gesellschaft auch deren allgemeiner Werbeauftritt, insbesondere auf der Website des Unternehmens. Insgesamt verbietet es sich in Zukunft, neben dem für einen Wettbewerbsverstoß verantwortlichen Unternehmen unreflektiert immer auch den Geschäftsführer in Anspruch zu nehmen, wie dies in der Vergangenheit im Wettbewerbsrecht teilweise gängige Praxis war. Es wird aber natürlich weiterhin Fälle geben, in denen dies nach wie vor aussichtsreich, sinnvoll oder gar erforderlich erscheint (etwa bei einer Ein-Personen-GmbH, die nur zur Haftungsabschirmung des Gesellschafter-Geschäftsführers für ein auf Rechtsverletzung ausgelegtes Geschäftsmodell gegründet wurde und jederzeit aufgegeben werden kann, oder bei naheliegender Möglichkeit der Verlagerung des wettbewerbswidrigen Verhaltens auf andere Unternehmen derselben Gruppe unter identischer Geschäftsführung). All dies gilt für Wettbewerbsverletzungen; geht es hingegen um Schutzrechtsverletzungen (z. B. Marken-, Patent- oder Designrechtsverletzungen), dürfte nach der Begründung des BGH weiterhin eine (Störer-) Haftung des Geschäftsführers schon dann bestehen, wenn er die Rechtsverletzung kannte und nichts dagegen unternommen hat.

EuGH: Keine öffentliche Wiedergabe eines Werks allein durch „Framing“

EuGH, Beschluss vom 21.10.2014 (Rs. C-348/13)

Oliver Brock
Rechtsanwalt
Standort: Düsseldorf
o.brock@heuking.de

Leitsatz:

Die Einbettung eines auf einer Website öffentlich zugänglichen geschützten Werkes in eine andere Website mittels eines Links unter Verwendung der Framing-Technik, wie sie im Ausgangsverfahren in Frage steht, allein stellt keine öffentliche Wiedergabe im Sinne von Art. 3 Abs. 1 der Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft dar, soweit das betreffende Werk weder für ein neues Publikum noch nach einem speziellen technischen Verfahren wiedergegeben wird, das sich von demjenigen der ursprünglichen Wiedergabe unterscheidet.

Anmerkung: Auf Vorlagefrage des BGH hatte sich der EuGH mit der Frage auseinanderzusetzen, ob die nicht genehmigte Wiedergabe eines Films über sog. „Framing“ im Internet gegen urheberrechtliche Verwertungsrechte verstößt. Beim „Framing“ werden Inhalte, die auf einer anderen Webseite abrufbar bereitgehalten werden, über einen Link in einem auf der abgerufenen Webseite erscheinenden Rahmen („Frame“) zugänglich gemacht. Bei einem Klick auf den Link wird der Inhalt dann abgespielt. Der Besucher der Webseite hat den Eindruck, dass der Inhalt auf der besuchten Webseite abgerufen wird. Im Ausgangsfall hatte ein Unternehmen einen kurzen Clip zum Thema Wasserverschmutzung herstellen lassen. Dieser wurde auf „YouTube“ hochgeladen, wobei das Unternehmen geltend macht, dass dies ohne seine Zustimmung erfolgt sei. Zwei selbstständige Handelsvertreter eines Wettbewerbers hatten das Video im Wege des „Framing“ dann auf ihrer eigenen Seite zugänglich gemacht. Darauf wurden sie abgemahnt und gaben eine Unterlassungserklärung ab. Der weitere Rechtstreit hat Schadensersatz und die Erstattung von Rechtsverfolgungskosten zum Gegenstand.

„Framing“ keine öffentliche Zugänglichmachung gemäß § 19a UrhG

Die Wiedergabe des Films, urheberrechtlich eines „Werks“, mit Hilfe des „Framings“ auf den Webseiten der Handelsvertreter stellte nach Auffassung des BGH keine öffentliche Zugänglichmachung i.S.d. § 19a UrhG dar. Die bisherige Rechtsprechung hatte hierzu vor allem das „normale“ Setzen eines Hyperlinks

zum Thema. Eine solche Linksetzung ist vom Wortlaut her zwar eine „Zugänglichmachung". Eine urheberrechtlich relevante Nutzungshandlung liegt aber nicht vor. Der Inhalt ist nämlich bereits auf der Webseite, auf die verwiesen wird, zugänglich gemacht worden. Der Linksetzer hat auch keine Kontrolle über die Bereithaltung der Inhalte. Dies gilt nach Ansicht des BGH im Vorlagebeschluss in Übereinstimmung mit der herrschenden Literaturmeinung auch für das bisher höchstrichterlich noch nicht behandelte „Framing". Auch hier liege die Kontrolle über die Bereithaltung des Werks nicht beim Linksetzer. Für die Frage, ob eine öffentliche Zugänglichmachung i.S.d. § 19a UrhG vorliege, sei auch der bloße Eindruck beim Nutzer irrelevant, das Werk werde auf der verlinkenden Internetseite wiedergegeben. Instanzgerichte wie das OLG Düsseldorf hatten dies noch anders gesehen und eine Verletzung des § 19a UrhG angenommen. Eine andere Bewertung nehmen BGH und EuGH bei Unterschieden im Detail bei der Setzung bestimmter „Deep Links" vor, bei denen der Linksetzer technische bzw. beschränkende Schutzmaßnahmen des Rechteinhabers umgeht.

„Framing" als Eingriff in sonstiges Verwertungsrecht?

Das Recht zur öffentlichen Zugänglichmachung nach § 19a UrhG ist aber nur eine besondere Ausprägung des Rechts zur öffentlichen Wiedergabe eines Werks nach § 15 Abs. 2 UrhG. Neben den benannten Verwertungsrechten der §§ 15 Abs. 2, 19 ff. kommt auch die Annahme eines unbenannten Rechts der öffentlichen Wiedergabe in Betracht (Innominatsrecht). Das Gesetz ist hier flexibel, um neue Nutzungsarten erfassen zu können und dem „Hinterherhinken" der Legislative bei technischen oder wirtschaftlichen Entwicklungen entgegenwirken zu können. Hierzu zählen z. B. das Abrufübertragungsrecht oder das Online-Verbreitungsrecht.

Nach Auffassung des BGH könnte die Wiedergabe eines Filmes durch „Framing" gegen ein solches unbenanntes Nutzungsrecht verstoßen. Bei dem Recht der öffentlichen Wiedergabe handelt es sich um ein sogenanntes harmonisiertes Recht. Es ist unionsrechtlich in Artikel 3 Abs. 1 der Informationsgesellschaftsrichtline (Richtlinie 2001/29) geregelt. Diese Vorschrift gilt zwar nicht unmittelbar. Das dort begründete Schutzniveau darf aber durch den nationalen Gesetzgeber weder über- noch unterschritten werden. Bei einer richtlinienkonformen Auslegung des § 15 Abs. 2 UrhG hätte nach Ansicht des BGH für die Annahme der Verletzung eines unbenannten Verwertungsrechts gesprochen, dass sich der Linksetzer das Werk durch seine Einbettung in die

eigene Internetseite zu eigen mache und sich die Zustimmung des Rechteinhabers für das eigene Bereithalten so erspare. Der Linksetzer hätte in diesem Fall eine zentrale Rolle bei der Werkvermittlung vergleichbar dem Setzer eines „Deep Links".

Wiedergabe mit „Framing" allein keine öffentliche Wiedergabe

Der EuGH hatte sich schon im Februar 2014 in der Rechtssache Svensson u. a./Retriever Sverige (Urteil vom 13.2.2014 – C-466/12) mit der Frage auseinanderzusetzen, ob das Setzen eines normalen „Hyperlinks" auf eine andere Webseite eine öffentliche Wiedergabe im Sinne des Artikel 3 Abs. 1 Informationsgesellschaftsrichtlinie darstellt. Soweit die Inhalte auf der verlinkten Seite frei zur Verfügung gestellt wurden, wurde die Frage verneint. Der BGH hielt trotzdem aufgrund der vermeintlichen Besonderheiten des „Framing" die Vorlagefrage aufrecht.

Der EuGH bestätigte nunmehr in Beschlussform, dass das „Framing" allein keine öffentliche Wiedergabe darstellt. Ein förmliches Urteil sei nicht erforderlich, da sich die Beantwortung der Vorlagefragen aus der bisherigen Rechtsprechung und insbesondere des Svensson u. a./Retriever Sverige-Urteils klar ergebe. Hiernach ist eine Verlinkung auch auf ein frei zugängliches Werk zwar eine Wiedergabe. Hier unterscheidet sich der EuGH von der bisherigen Rechtsprechung des BGH, der schon grundsätzlich keine urheberrechtlich relevante Nutzungshandlung annahm. Öffentlichkeit liegt aber nicht vor. Diese setzt voraus, dass das Werk entweder unter Verwendung eines anderen technischen Verfahrens oder für ein neues Publikum, das sich von dem ursprünglich vorgesehenen Publikum unterscheidet, wiedergegeben wird. Die Annahme eines anderen technischen Verfahrens scheidet bei der Verlinkung aus, da die Übertragung im Internet jeweils gleich leitungsgebunden mit Hilfe des IP-Protokolls erfolgt. Bleibt die Frage, ob ein neues Publikum erreicht wird.

Dies sei beim „Framing" jedenfalls dann nicht der Fall, wenn das Werk auf der verlinkten Webseite frei zugänglich ist. Machen die Rechteinhaber ihr Werk im Internet frei für alle Internetnutzer zugänglich, seien auch die Besucher der verlinkenden Seite ursprünglich intendiertes und kein neues Publikum. Insbesondere komme es nicht auf die Frage an, ob sich der Linksetzer das Werk zu eigen mache und den Eindruck erwecke, das Werk sei in Wirklichkeit Teil der eigenen Webseite. Es sei auch nicht entscheidend, ob das „Framing" geeignet sei, gerade die Notwendigkeit einer Kopie des Werkes zu vermeiden.

Der neuerliche Beschluss des EuGH wäre nach dem Svensson u. a./Retriever Sverige-Urteil eigentlich nicht notwendig gewesen, die grundsätzlichen Erwägungen zu „Hyperlinks" dort waren problemlos auf das „Framing" zu übertragen. Jetzt ist aber unionsrechtlich die Gleichbehandlung von „Hyperlinks" und „Framing" im Rahmen des Artikel 3 Abs. 1 Informationsgesellschaftsrichtlinie bestätigt. Das Urteil vom Februar und der nochmalige Beschluss vom Oktober 2014 haben aber potentiell aus anderen Gründen Sprengkraft und werfen Fragen auf. Der EuGH weicht hier mit der grundsätzlichen Annahme einer urheberrechtlich relevanten Nutzungshandlung bei der Linksetzung auf ein frei zugängliches Werk fundamental von der bisherigen deutschen „Paperboy"-Rechtsprechung (BGH GRUR 2003, 958, 962 – Paperboy) ab. Da die Frage des „neuen Publikums" damit verbunden ist, ob der Rechteinhaber bei der Erstverwertung an das weitere Publikum gedacht hat, stellt sich die Frage, wie mit den Fällen zu verfahren ist, bei denen das Werk ohne Erlaubnis des Rechteinhabers in die Öffentlichkeit gelangt ist. Auch ist ein Unternehmen, das Inhalte auf seiner eigenen Internetpräsenz bereithält, möglicherweise gerade daran interessiert, dass sich der Nutzer dort und nicht woanders informiert.

Fazit: Die Annahme, dass bei Fehlen einer technischen Beschränkung des Zugriffs auf Inhalte von der Zustimmung zu jeder erdenklichen Nutzung im Internet auszugehen ist, ist eine faktisch kaum haltbare Fiktion. Für das Internet bedeutet dies, dass das Merkmal der „neuen Öffentlichkeit" stets bei Nichtvorliegen von Schutzmaßnahmen zu verneinen wäre. In diesem Fall ist dann der Rechteinhaber wiederum völlig schutzlos. So weit geht der EuGH dann auch nicht. Ausdrücklich wird festgestellt, dass es jenseits der zwei „Regelbeispiele" auch noch in anderen Fällen zu einer lizenzpflichtigen Verwertungshandlung i. S. einer öffentlichen Wiedergabe kommen kann, aber eben nicht „allein" durch die Einbettung. Es bleibt also auch weiterhin Raum für eine Gesamtbetrachtung aller Umstände, in der etwa die Frage, ob die betreffende Nutzungshandlung Erwerbszwecken dient, eine Rolle spielen kann.

Aus unserer Praxis
IP, Media & Technology

Veröffentlichungen

Dr. Dirk Stolz und **Dr. Lutz Keppeler** (beide Köln) haben in der soeben im Verlag der Global Legal Group Ltd. erschienenen 8. Auflage von „The International Comparative Legal Guide to: Telecoms, Media & Internet Laws & Regulations 2015" das Länderkapitel für Deutschland verfasst (ICLG 2015, 110).

Michael Schmittmann und **Oliver Brock** (beide Düsseldorf) haben in der von Professor Dr. Rolf Schwartmann herausgegebenen und im C.F. Müller Verlag im August 2014 erschienenen 3. Auflage des „Praxishandbuchs Medien-, IT- und Urheberrecht" das Kapitel Telemedienrecht grundlegend neu bearbeitet.

Dr. Georg Jacobs, LL.M. (Düsseldorf) kommentiert in dem soeben im C.H. Beck Verlag neu erschienenen „Prozesskommentar zum Gewerblichen Rechtsschutz" von Cepl/Voß die §§ 214 bis 238 ZPO.

Außerdem hat **Dr. Georg Jacobs, LL.M.** (Düsseldorf) in der Fachzeitschrift GRUR-Prax vier Entscheidungsbesprechungen veröffentlicht, nämlich eine Urteilsanmerkung zu der Entscheidung BGH, Urteil vom 17.7.2013, Az. I ZR 52/12 betreffend die „Freie Benutzung einer literarischen Figur durch Übernahme nur äußerer Merkmale" (GRUR-Prax 2014, 39), eine Besprechung der Entscheidung BGH, Urteil vom 19.2.2014, Az. I ZR 230/12 betreffend einen „Betriebsversuch zur Beweisaufnahme mit verschwiegenem Sachverständigen" (GRUR-Prax 2014, 212), eine Anmerkung zu der Entscheidung LG Köln, Urteil vom 16.4.2014, Az. 84 O 33/14 betreffend „Wettbewerbliche Eigenart wegen Farbe" (GRUR-Prax 2014, 339) sowie eine Anmerkung zu der Entscheidung BGH, Beschluss vom 3.4.2014, Az. I ZB 6/12 betreffend eine „Rechtsbeschwerde wegen pflichtwidriger Nicht-Vorlage zum EuGH – Schwarzwälder Schinken" (GRUR-Prax 2014, 433).

Kai Runkel (Köln) hat in der Fachzeitschrift Medien und Recht International eine Besprechung der Entscheidung BGH, Urteil vom 13.11.2013, Az. I ZR 143/12 – „Geburtstagszug" (betreffend die erforderliche Schöpfungshöhe für den Urheberrechtsschutz bei Werken angewandter Kunst) veröffentlicht (MR-Int 2013, 82).

In der Fachzeitschrift Der IP-Rechtsberater ist ein Beitrag von **Thorsten Wieland** (Frankfurt a. M.) mit dem Titel „Markenrechtliche Erschöpfung und Vertrieb von Produktfälschungen – Eine Momentaufnahme aus der Rechtsdurchsetzung" erschienen (IPRB 2014, 209).

Vorträge

Auf der INTA-Konferenz „Branding & Social Media" in Chicago, USA, beleuchtete **Dr. Søren Pietzcker** (Hamburg) im Rahmen eines Vortrags zum Thema „Building an International trademark protection program for brands in a global digital environment" neue Entwicklungen im Bereich Social Media.

Im November 2013 hielt **Dr. Søren Pietzcker** (Hamburg) auf der Promotion and Marketing Law Conference in Chicago, USA, einen Vortrag zum Thema „Globalizing your marketing strategies".

Oliver Brock (Düsseldorf) hielt im Juni 2014 auf der IFLCA (International Federation of Computer Law Associations)-Konferenz in Antwerpen einen Vortrag zum Thema „Multiscreen, Catch-up & OTT – how about rights acquisition?".

Im August 2014 referierte **Dr. Lutz M. Keppeler** (Köln) im Rahmen des BITKOM Akademie Workshops „Smart Home – Wird endlich gut, was (sehr) lange währt?" zu dem Thema „Sensoren und Netze hautnah in der Wohnung: Was sagt der Datenschutz?".

Astrid Luedtke (Düsseldorf) hat am 2. Juni 2014 in Wiesbaden im Rahmen des Seminars „Update Datenschutz – Datenschutz in der Medizin" zu Datenpannen im Gesundheitsbereich vorgetragen.

Am 3., 10. und 17. September 2014 haben **Dr. Ruben Hofmann** (Köln), **Astrid Luedtke** (Düsseldorf) und **Dr. Andreas Walle** (Hamburg) in Kooperation mit dem Bund der Unternehmensjuristen e. V. (BUJ) das Seminar „Social Media und Ihr Unternehmen – Chancen und Risiken der Nutzung" in Hamburg, Berlin und Frankfurt a. M. gehalten.

Zu Rechtsfragen rund um das Thema Datenschutz in digitalen Medien referierte **Dr. Søren Pietzcker** (Hamburg) im Rahmen des Seminars „TV and Social Media Advertising – a legal perspective" im September 2014 in Stockholm/Schweden zum Thema „Data Protection and Advertising in Digital Media".

Anlässlich des Software Freedom Days hielt **Dr. Lutz M. Keppeler** (Köln) im September 2014 einen Vortrag zu der Frage: „Lizenzkonflikte bei der Kombination verschiedener Open-Source-Lizenzen als ‚tickende Zeitbombe' des Informationszeitalters?"

Auszeichnungen

JUVE Awards: Heuking Kühn Lüer Wojtek ist Kanzlei des Jahres für Informationstechnologie

JUVE 2014 AWARDS
Kanzlei des Jahres für Informationstechnologie

Bei der Verleihung der JUVE Awards am 23. Oktober 2014 wurde Heuking Kühn Lüer Wojtek als „Kanzlei des Jahres für Informationstechnologie" ausgezeichnet. Wie sich aus der Begründung dieser Entscheidung durch JUVE ergibt, waren hierfür insbesondere die Tätigkeit des Teams um **Dr. Stephan Witteler** (Frankfurt a. M.) im Rahmen des „Herkules"-Projekts der Bundeswehr, die Begleitung des Aufbaus der IPTV-Vertriebsplattform „Mein Fernsehen" des Satellitenbetreibers Eutelsat durch unser Düsseldorfer Team, die IT-Outsourcing-Beratung der Funke-Mediengruppe sowie der Ausbau unserer Beratungsfelder in den Bereichen Datenschutz und Cloud Computing ausschlaggebend.

Professor Rainer Jacobs zum Ehrenmitglied der GRUR ernannt

Professor Dr. Rainer Jacobs aus unserem Düsseldorfer Büro ist auf der letzten GRUR-Jahrestagung zum Ehrenmitglied der GRUR gewählt worden. Damit werden seine mehr als 30jährige Tätigkeit als Mitherausgeber der GRUR (zuständig für den Rechtsprechungsteil) und seine damit verbundenen Verdienste für die Deutsche Vereinigung für gewerblichen Rechtsschutz und Urheberrecht gewürdigt.

Personalien

Zuwachs in Düsseldorf

Isabel Skara
Rechtsanwältin
Standort: Düsseldorf
i.skara@heuking.de

Seit Oktober 2014 verstärkt **Isabel Skara** unsere Praxisgruppe am Düsseldorfer Standort und setzt damit das Wachstum des IT-Rechtsteams fort. Isabel Skara absolvierte ihre Anwaltsstation im Rahmen des Referendariats in einer renommierten, auf den Bereich des Gewerblichen Rechtsschutz spezialisierten Boutique in Düsseldorf. Nach dem zweiten Staatsexamen schrieb sie ihre Dissertation im Patentrecht und sammelte praktische Erfahrungen als wissenschaftliche Mitarbeiterin in einer internationalen Wirtschaftskanzlei im Bereich Gewerblicher Rechtsschutz. Isabel Skara unterstützt Michael Schmittmann, Astrid Luedtke, Dr. Philip Kempermann und Oliver Brock in den Bereichen Informationstechnologie und Medienrecht.

Zuwachs in Frankfurt a. M.

Christine Grau, LL.M.
Rechtsanwältin
Standort: Frankfurt a. M.
c.grau@heuking.de

Seit Dezember 2013 ist **Christine Grau, LL.M.** an unserem Frankfurter Standort tätig und setzt damit das Wachstum des Technologyteams fort. Nach dem zweiten Staatsexamen erwarb sie den Titel LL.M. im Bereich Internationales Recht. Sie war zunächst als juristische Referentin im GSI Helmholtzzentrum für Schwerionenforschung GmbH tätig und beriet dort die Bereiche Forschung und IT sowie die Patentabteilung. Christine Grau unterstützt das Dezernat von Dr. Stephan Witteler in den Bereichen Informationstechnologie und Telekommunikationsrecht.

Dr. Ubbo Aßmus
Rechtsanwalt
Standort: Frankfurt a. M.
u.assmus@heuking.de

Seit April 2014 verstärkt **Dr. Ubbo Aßmus** das IT-Team an unserem Standort in Frankfurt a. M. Dr. Ubbo Aßmus studierte Rechtswissenschaften an den Universitäten Dresden, Helsinki und Freiburg im Breisgau. Nach seinem ersten Staatsexamen absolvierte er sein Referendariat in Düsseldorf und Berlin. Im Anschluss daran arbeitete er als wissenschaftlicher Mitarbeiter an der Universität Mannheim. Parallel dazu promovierte er bei Prof. Dr. Alexander Roßnagel zu einem datenschutzrechtlichen Thema. Von 2012 bis 2014 arbeitete Dr. Aßmus als Rechtsanwalt im Bereich Gesellschaftsrecht und IT-Recht als Associate bei Weil, Gotshal & Manges LLP in Frankfurt am Main. Im Herbst 2013 wurde er zum Dr. jur. promoviert. Seit April 2014 arbeitet

Dr. Aßmus bei Dr. Stephan Witteler am Frankfurter Standort von Heuking Kühn Lüer Wojtek. Dort ist er in den Bereichen IT-Recht, Gesellschaftsrecht sowie Vertragsrecht tätig.

Moritz Schönpflug, LL.M.
Rechtsanwalt
Standort: Frankfurt a. M.
m.schoenpflug@heuking.de

Moritz Schönpflug, LL.M., ist im April 2014 zu unserer Praxisgruppe am Standort Frankfurt am Main gestoßen. Er verstärkt dort das Team um Thorsten Wieland. Sein Tätigkeitsgebiet umfasst insbesondere die Bereiche Produktpiraterie und Wettbewerbsrecht. Erste Einblicke in den Gewerblichen Rechtsschutz erhielt Moritz Schönpflug während des Schwerpunktbereichsstudiums an den Universitäten Bayreuth und Bonn. Seine Kenntnisse in dem Bereich vertiefte er im Anschluss an die Erste Juristische Prüfung während seiner Mitarbeit am Lehrstuhl für das Geistige Eigentum an der Rheinischen Friedrich-Wilhelms-Universtität Bonn, seines LL.M.-Studiums im Bereich IP an der Benjamin N. Cardozo School of Law in New York City sowie im Rahmen seiner Ausbildung im Soft und Hard IP bei auf IP Litigation spezialisierten Wirtschaftskanzleien.

Zuwachs in Köln

Dr. Lutz Martin Keppeler
Rechtsanwalt
Standort: Köln
l.keppeler@heuking.de

Seit April 2014 ist **Dr. Lutz Martin Keppeler** am Kölner Standort unserer Sozietät tätig und verstärkt dort vor allem die IT- und datenschutzrechtliche Praxis. Während seines Studiums an der Universität zu Köln absolvierte Lutz M. Keppeler den Schwerpunktbereich Medienrecht. Nach einem Auslandssemester in La Coruña verfasste er eine zivilrechtliche Doktorarbeit mit rechtshistorischen und rechtsphilosophischen Bezügen und wurde hierfür 2013 mit dem Fakultätspreis der Universität zu Köln ausgezeichnet. Während der Erstellung der Doktorarbeit und des Referendariats arbeitete Lutz M. Keppeler als wissenschaftlicher Mitarbeiter an der Universität zu Köln, bei Heuking Kühn Lüer Wojtek und in verschiedenen internationalen Großkanzleien. Bevor er erneut zu Heuking Kühn Lüer Wojtek kam, arbeitete er als Anwalt bei Clifford Chance. Lutz M. Keppeler unterstützt Dr. Dirk Stolz und Dominik Eickemeier in den Bereichen IT- und Datenschutzrecht.

Seit Juni 2014 verstärkt **Dr. Stefanie Langen** unsere Praxisgruppe am Münchner Standort. Sie studierte an den Universitäten Bonn, Köln und San Diego (USA). Dabei belegte sie den Schwerpunkt „Geistiges Eigentum und Wettbewerb" und arbeitete neben ihrem Studium bei einer überörtlichen Rechtsanwaltssozietät in Köln. Im Anschluss an die erste juristische Staatsprüfung war sie als wissenschaftliche Mitarbeiterin am Institut für Gewerblichen Rechtsschutz und Urheberrecht an der Universität zu Köln tätig und promovierte dort über ein wettbewerbsrechtliches Thema. Während ihres Referendariats arbeitete Stefanie Langen als wissenschaftliche Mitarbeiterin bei einem Kölner Internetunternehmen im Bereich Markenrecht. Ihr Referendariat umfasste Stationen beim Bildungsministerium in Sydney (Australien) sowie in internationalen Wirtschaftskanzleien in Köln und Düsseldorf. Nach dem Berufseinstieg bei einer internationalen Wirtschaftskanzlei in München wechselte Stefanie Langen zu Heuking Kühn Lüer Wojtek und unterstützt seitdem Dr. Ulrike Helkenberg im Bereich Gewerblicher Rechtsschutz.

Zuwachs in München

Dr. Stefanie Langen
Rechtsanwältin
Standort: München
s.langen@heuking.de

HEUKING KÜHN LÜER WOJTEK

www.heuking.de

Redaktion:
Rechtsanwalt Marc Oliver Brock, Düsseldorf
Rechtsanwalt Kai Oliver Runkel, Köln

Verantwortlicher Redakteur:
Rechtsanwalt Kai Runkel
bei der PartGmbB von Rechtsanwälten und Steuerberatern
Heuking Kühn Lüer Wojtek,
Magnusstraße 13, 50672 Köln

Diese und alle weiteren Ausgaben des Newsletters IP, Media & Technology finden Sie im Internet unter www.heuking.de/ueber-uns/newsletter.html.

Berlin
Unter den Linden 10
10117 Berlin
T +49 30 88 00 97-0
F +49 30 88 00 97-99

Hamburg
Neuer Wall 63
20354 Hamburg
T +49 40 35 52 80-0
F +49 40 35 52 80-80

Chemnitz
Weststraße 16
09112 Chemnitz
T +49 371 38 203-0
F +49 371 38 203-100

Köln
Magnusstraße 13
50672 Köln
T +49 221 20 52-0
F +49 221 20 52-1

Düsseldorf
Georg-Glock-Straße 4
40474 Düsseldorf
T +49 211 600 55-00
F +49 211 600 55-050

München
Prinzregentenstraße 48
80538 München
T +49 89 540 31-0
F +49 89 540 31-540

Brüssel
Rue Froissart 95
1040 Brüssel/Belgien
T +32 2 646 20-00
F +32 2 646 20-40

Frankfurt
Goetheplatz 5-7
60313 Frankfurt am Main
T +49 69 975 61-415
F +49 69 975 61-200

Stuttgart
Augustenstraße 1
70178 Stuttgart
T +49 711 22 04 579-0
F +49 711 22 04 579-44

Zürich
Bahnhofstrasse 3
8001 Zürich/Schweiz
T +41 44 200 71-00
F +41 44 200 71-01

RECHTSANWÄLTE UND STEUERBERATER