Luther.

IP/IT

(Intellectual Property/Information Technology)

Das neue EU-U.S. Privacy Shield tritt in Kraft

Freies WLAN für alle?

Know-how-Richtlinie: Compliance auf dem Prüfstand

Die künstlerische Gestaltung kann einen Eingriff in Urheber- und Leistungsschutzrechte rechtfertigen

„Internetpranger"

Weitere Themen im Innenteil

Newsletter 3. Ausgabe 2016

Das neue EU-U.S. Privacy Shield tritt in Kraft

Auf den Punkt.
Am 12. Juli 2016 wurde die Nachfolgeregelung für das im Oktober 2015 vom EuGH in der Sache Maximillian Schrems v. Data Protection Commissioner (C-362/14) gekippte Safe Harbor Abkommen mit nur wenigen punktuellen Änderungen durch die Europäische Kommission formell verabschiedet. Das Privacy Shield kann zukünftig, vorbehaltlich der Anerkennung durch die nationalen Aufsichtsbehörden, zur Legitimation eines Datentransfers in die USA herangezogen werden. Allerdings ist eine baldige erneute Überprüfung durch den EuGH zu erwarten.

Hintergrund

Im Herbst 2015 hatte der EuGH das sog. Safe Harbor Abkommen, auf dessen Grundlage europäische Unternehmen personenbezogene Daten in die USA übermitteln durften, für ungültig erklärt, weil es keine hinreichende Garantie für den Schutz der übermittelten Daten vor u.a. unerlaubten Zugriffen durch US-Behörden gewährleistete. Der im Februar 2016 vorgelegte Entwurf einer Nachfolgeregelung war scharf kritisiert worden (vgl. unseren Beitrag in Ausgabe 2/2016). Trotz der heftigen Kritik wurde das Privacy Shield am 12. Juli 2016 mit nur wenigen punktuellen Änderungen durch die Europäische Kommission formell verabschiedet. Zuvor hatten am 8. Juli 2016 die EU-Mitgliedsstaaten in der sog. Art. 31 Gruppe nach anfänglicher Zurückhaltung letztlich doch mehrheitlich ihre Zustimmung zu der Nachfolgeregelung erteilt.

Hohes Datenschutz-Niveau durch das neue Privacy Shield?

Nach Meinung der Europäischen Kommission vom 8. Juli 2016 (http://europa.eu/rapid/press-release_STATEMENT-16-2443_en.htm) gewährleistet das neue EU-U.S. Privacy Shield ein hohes Datenschutzniveau zugunsten betroffener Personen sowie Rechtssicherheit für datenverarbeitende Unternehmen. Das Privacy Shield unterscheide sich fundamental von der Vorgängerregelung Safe Harbor, da es datenverarbeitenden Unternehmen in den USA klare und verbindliche Vorgaben zum Umgang mit den Daten auferlege und für deren Kontrolle und Durchsetzung sorge. Zudem habe die USA erstmalig schriftlich zugesagt, dass öffentliche Stellen, einschließlich Geheimdienste, nur unter bestimmten engen Voraussetzungen auf personenbezogene Daten europäischer Bürger zugreifen dürfen und eine willkürlich Massenüberwachung ausgeschlossen sei.

Ob die jetzt verabschiedete Version des Privacy Shields künftig tatsächlich ein angemessenes Schutzniveau in den USA gewährleisten kann, darf jedoch bezweifelt werden. Denn trotz punktueller Nachbesserungen dürfte der Mehrwert des Nachfolgeabkommens eher gering sein. Zwar entsprechen die ausgehandelten Standards europäischen Anforderungen an einen ausreichenden Datenschutz. Auch ist eine stärkere Kontrolle der Einhaltung der Vorschriften und Sanktionierung von Verstößen vorgesehen. Jedoch ändert das neue Abkommen nichts an der geltenden Gesetzeslage in den USA, die Ermittlungsbehörden und Geheimdiensten umfangreiche Überwachungsbefugnisse einräumt. Zudem sieht das Privacy Shield explizit Ausnahmen für die zwingende Befolgung der neuen Datenschutzstandards vor, nämlich u.a. soweit ein Gesetz dies erlaubt oder die Missachtung der Grundsätze aus Gründen der nationalen Sicherheit, zum Zwecke der Rechtsdurchsetzung oder aus anderen öffentlichen Interessen erforderlich ist. Da hilft es auch wenig, wenn die USA der Europäischen Kommission schriftlich zusagen, dass eine willkürliche Massenüberwachung europäischer Bürger zukünftig nicht mehr stattfinde, denn der Begriff der „Überwachung“ wird durch europäische und US-amerikanische Stellen bereits grundlegend unterschiedlich definiert: Die USA halten eine „bulk collection“ von Daten für zulässig (auch wenn eine gezielte Datenerhebung in Bezug auf konkrete Einzelpersonen die Regel sein soll) und beschränken erst die eigentliche Auswertung der Daten. Nach europäischem Datenschutzrecht unterliegen hingegen bereits die Erhebung und Speicherung der Daten dem strengen Erlaubnisvorbehalt und Zweckbindungsgrundsatz. Auf der Grundlage des Foreign Intelligence Surveillance Acts (FISA) oder der National Security Letters kann daher auch zukünftig eine umfangreiche Erhebung und Auswertung personenbezogener Daten europäischer Personen stattfinden.

Unser Kommentar

Theoretisch kann ab sofort auf das neue Privacy Shield zur Legitimation von Datentransfers in die USA zurückgegriffen werden. Indes ist es nationalen Aufsichtsbehörden mög-

lich, Datentransfers auf dieser Grundlage zu untersagen, wenn sie im Rahmen ihrer Kontrollbefugnisse zu der Ansicht gelangen, dass ein hinreichendes Schutzniveau tatsächlich nicht gewährleistet ist. Diese Kompetenz hat der EuGH den nationalen Aufsichtsbehörden in seinem o.g. Urteil ausdrücklich zugesprochen. Aufgrund des weiterhin starken Misstrauens gegenüber der Effektivität des neuen Schutzschilds besteht zudem die Gefahr, verschärft in den Fokus der Aufsichtsbehörden zu gelangen, wenn Unternehmen Datentransfers alleine auf diese Grundlage stützen. Zudem ist es wahrscheinlich, dass sich der EuGH schon bald erneut mit der Frage der Wirksamkeit des Privacy Shields auseinandersetzen werden muss, sodass eine (zusätzliche) Rechtsgrundlage in Form etwa der EU-Standardvertragsklauseln oder der Binding Corporate Rules weiterhin zu empfehlen ist.

Freies WLAN für alle?

Auf den Punkt.

Die Abschaffung der Störerhaftung ist beschlossen. Denn am 2. Juni hat der Deutsche Bundestag das Zweite Gesetz zur Änderung des Telemediengesetzes verabschiedet. Bereits im Herbst könnten die Änderungen in Kraft treten, sodass Betreiber öffentlicher WLAN-Netze nicht mehr Gefahr laufen, wegen eines rechtswidrigen Verhaltens ihrer Nutzer abgemahnt zu werden. Damit ist der Weg frei für flächendeckend offene WLAN-Netze.

Hintergrund des Gesetzes: Deutschland als „Hot-Spot-Wüste“

Was in weiten Teilen der Welt seit Langem Normalität ist, ist in Deutschland noch immer eine Seltenheit: Freie WLAN-Netze. Laut einer Erhebung von eco (dem Verband der deutschen Internetwirtschaft e. V.) kommen auf 10.000 Einwohner gerade einmal 1,9 offene WLAN-Hotspots. Zum Vergleich: In den USA sind es 4,8, in Schweden 9,9, in Großbritannien stolze 28,7, was nur noch von Südkorea mit 37,4 übertroffen wird. Bislang sind in Deutschland vor allem die Haftungsrisiken für potentielle Betreiber von WLAN-Hotspots aufgrund der sogenannten „Störerhaftung“ ein wesentliches Hindernis. Denn bislang mussten auch private Betreiber von Hotspots aufgrund der Störerhaftung für das Fehlverhalten ihrer Nutzer haften. Diese Störerhaftung soll nach langem Streit in der großen Koalition nun möglichst schnell durch Änderungen des Telemediengesetzes (TMG) abgeschafft werden.

Störerhaftung – ein deutsches Phänomen

Ob ein Betreiber von WLAN-Internetzugängen für Rechtsverletzungen seiner Nutzer haften muss, ist gesetzlich bislang nicht eindeutig geregelt. Seit einem Urteil des Bundesgerichtshofs (BGH) vom 12. Mai 2010 (Az.: I ZR 121/08, „Sommer unseres Lebens“) gilt in Deutschland jedoch die Störerhaftung für die Betreiber von Internetzugängen. Danach kann ein (privater) Anschlussinhaber für Rechtsverstöße Dritter auf Unterlassung in Anspruch genommen werden, wenn der Dritte unter Nutzung des Internetzugangs Rechtsverletzungen (bspw. den Download eines urheberrechtlich

geschützten Werkes) begeht. Die Störerhaftung setzt an der Ermöglichung der Rechtsverletzung an; mit der Störerhaftung kann somit auch derjenige belangt werden, der nur die Internetverbindung bereitgestellt hat, ohne die Rechtsverletzung selbst zu begehen. Dies gilt insbesondere dann, wenn der Anschlussinhaber die Nutzung des Internetzugangs durch dritte Personen nicht überwacht oder keine Maßnahmen getroffen hat, um illegalen Handlungen vorzubeugen.

Offene WLAN-Netze ohne Passwort oder eine vorgeschaltete Seite sind deshalb hierzulande eine Seltenheit. Kleinere Unternehmen wie Cafés oder Hotels verzichten lieber auf offene Netze (und damit auch auf potentielle Kunden) als sich dem Risiko von Abmahnungen wegen Rechtsverstößen über den Internetanschluss auszusetzen. Mit der Neuregelung soll nach dem Willen der Bundesregierung das Hemmnis der möglichen Haftung ausgeräumt und so der Weg zu einer größeren WLAN-Abdeckung in Deutschland geebnet werden.

Rückenwind aus Luxemburg

Für die Abschaffung der Störerhaftung mitverantwortlich ist auch ein Gutachten des Generalanwaltes am Europäischen Gerichtshof (EuGH) Maciej Szpunar aus März 2016, wonach Betreiber eines Geschäfts, die kostenlos der Öffentlichkeit ein WLAN-Netz zur Verfügung stellen, für Urheberrechtsverletzungen eines Dritten nicht verantwortlich gemacht werden können. Diese Auffassung vertrat jedenfalls der Generalanwalt in seinen Schlussanträgen in der Vorabentscheidungssache Rs. C-484/14 vor dem EuGH. In diesem Fall ging es um einen Licht- und Tontechnik-Vermieter aus München, der über sein Geschäft ein öffentlich zugängliches WLAN-Netz bereitstellte. Über diesen Internetanschluss wurden rechtswidrig urheberrechtlich geschützte Musikwerke zum Download angeboten. In dem Gerichtsverfahren zwischen dem Anschlussinhaber und der Rechteinhaberin ging das zunächst mit der Sache befasste LG München I zwar davon aus, dass der Anschlussinhaber nicht selbst die betreffenden Urheberrechte verletzt habe, es hielt eine mittelbare Haftung des Anschlussinhabers als Störer jedoch für denkbar, da dieser sein WLAN-Netz nicht gesichert hatte. Allerdings hatte das Gericht Zweifel, ob die dem deutschen Recht zugrundeliegende europäische Richtlinie 2000/31/EG über den elektronischen Geschäftsverkehr (sog. „E-Commerce-Richtlinie“) einer Störerhaftung entgegensteht. Denn nach Art. 12 Abs. 1 der E-Commerce-Richtlinie sind Vermittler, die Dienste der reinen Durchleitung von Daten anbieten, für rechtswidrige Handlungen Dritter nicht verantwortlich, sofern folgende drei Voraussetzungen kumulativ erfüllt sind: Der Diensteanbieter hat die Übermittlung nicht veranlasst, den Adressaten der Übertragung nicht ausgewählt und die übermittelten Informationen nicht ausgewählt oder verändert. Das Gericht setzte daher das Verfahren aus, um dem EuGH die Frage zur Vorabentscheidung vorzulegen, ob die in der E-Commerce-Richtlinie vorgesehene Haftungsbeschränkung auch für Personen gelte, die als Nebentätigkeit zu ihrer wirtschaftlichen Haupttätigkeit ein öffentliches WLAN-Netz kostenlos zur Verfügung stellen.

Nach Auffassung des Generalanwalts stehe Artikel 12 Abs. 1 der E-Commerce-Richtlinie (und damit auch die deutsche Umsetzung in § 8 Abs. 1 TMG) einer eigenen Haftung des Vermittlers entgegen. Das für „Access-Provider“ geschaffene Privileg gelte bei Einhaltung der genannten Voraussetzungen auch für andere Gewerbetreibende. Eine gerichtliche Anordnung, die darauf gerichtet ist, eine bestimmte Rechtsverletzung abzustellen oder zu verhindern, sei allerdings auch in Zukunft zulässig, soweit es dem Adressaten freistehe, welche konkreten Maßnahmen er dazu ergreift. Die Anordnung müsse zudem verhältnismäßig sein, weshalb sie nicht so weit gehen dürfe, dem Anschlussinhaber eine Stilllegung des Internetanschlusses, einen Passwortschutz oder die Überwachung der Kommunikation aufzugeben. Ob der EuGH (wie häufig) diesen Empfehlungen des Generalanwalts folgen wird, bleibt bis zu dem bald zu erwartenden Urteil abzuwarten.

Änderungen des TMG

Um künftig eine möglichst weitgehende Verbreitung von WLAN-Internetzugängen zu ermöglichen, sollen in Zukunft auch Privatpersonen das Haftungsprivileg des § 8 TMG genießen. Diensteanbieter nach § 8 TMG sind demnach alle WLAN-Betreiber unabhängig davon, ob sie ihr WLAN zu „kommerziellen Zwecken, im privaten Umfeld oder als öffentliche Einrichtung zur Verfügung stellen“ (Drucksache 18/6745, S.10). Die E-Commerce-Richtlinie, über deren Auslegung der EuGH zu entscheiden hat, setzt dagegen voraus, dass ein Anbieter im Sinne der Richtlinie eine Dienstleistung erbringt, die „in der Regel gegen Entgelt“ erbracht wird. Die einheitliche deutsche Regelung, die auch private Anbieter erfasst, geht damit sogar über die europäischen Vorgaben hinaus. Um Rechtssicherheit zu schaffen, stellt der neu gefasste § 8 Abs. 3 TMG nun klar, dass Anbieter von WLAN-Zugängen ohne jede Einschränkung Diensteanbieter im Sinne des § 8 TMG sind und somit dem Haftungsprivileg unterfallen. Die ursprüngliche Entwurfsfassung des Bundeswirtschaftsministeriums hatte in Anlehnung an die Rechtsprechung des BGH noch die Einschränkung vorgesehen, dass das Haftungsprivileg nur gelte, wenn der Internetzugang durch Passwort gesichert sei und der Nutzer erkläre, keine Rechtsverletzungen zu begehen. Darüber hinaus macht die Geset-

zesbegründung durch einen Verweis auf die Schlussanträge des Generalanwalts Szpunar deutlich, dass zukünftig kein Anbieter eines WLAN-Zugangs für Rechtsverstöße Dritter auf Zahlung von Schadensersatz, Gerichts- oder Abmahnkosten in Anspruch genommen werden kann.

Aktuelles BGH-Urteil zur Störerhaftung

Taucht ein urheberrechtlich geschütztes Werk in einer Tauschbörse auf, kann der Rechteinhaber, unter Zuhilfenahme von Abmahnkanzleien, die IP-Adresse des Anschlussinhabers ermitteln und diesen zur Abgabe einer Unterlassungserklärung sowie zur Zahlung von Schadensersatz und Abmahnkosten auffordern. Ist der Anschlussinhaber nicht der Täter der Rechtsverletzung, so haftet dieser dennoch aufgrund des Rechtsinstituts der Störerhaftung auf Unterlassung und Zahlung der Abmahnkosten, wenn der Anschlussinhaber seine sog. „Sicherungs- oder Belehrungspflichten“ missachtet hat. Mit Urteil vom 12. Mai 2016 (Az.: I ZR 86/15) hat auch der BGH nun die Störerhaftung von Anschlussinhabern eingeschränkt, indem es die anlasslose Belehrungs- und Überwachungspflicht gegenüber sämtlichen Mitnutzern des Internetanschlusses als "nicht sozialadäquat" bezeichnete. Demgemäß müssen volljährige Gäste, Besucher und Mitbewohner ohne besonderen Grund nicht über die rechtlichen Konsequenzen illegaler Downloads belehrt werden. Auch haftet der Anschlussinhaber nicht ersatzweise, wenn nicht festgestellt werden kann, wer die Urheberrechtsverletzung begangen hat.

Unser Kommentar

Die Abschaffung der Störerhaftung ist eine erfreuliche Nachricht für alle Betreiber öffentlicher WLAN-Netze, einschließlich Privatpersonen, die ihren Internetzugang Familienmitgliedern und Bekannten zur Nutzung zur Verfügung stellen. Es ist zu erwarten, dass die Gesetzesänderung und das noch zu erwartende Urteil des EuGH die flächendeckende Verbreitung von offenen WLAN-Netzen endlich vorantreiben wird.

Know-how-Richtlinie: Compliance auf dem Prüfstand

Auf den Punkt.

Bislang wurden in Deutschland Geschäftsgeheimnisse im Wesentlichen über das Wettbewerbsrecht (§§ 17, 18 UWG) und/oder geschlossene Vertraulichkeitsvereinbarungen geschützt. Das geltende Recht zum Schutz von Geschäftsgeheimnissen wird sich aber im Hinblick auf die kürzlich verabschiedete Know-how-Richtlinie ändern. Unternehmen sind daher aufgerufen, ihre Vertraulichkeitsvereinbarungen mit Kunden und Mitarbeitern auf deren Übereinstimmung mit der neuen EU-Richtlinie zu überprüfen und gegebenenfalls anzupassen.

Hintergrund und Umsetzungsfrist

Seit längerer Zeit wurde deutlich, dass die Regeln der Mitgliedsländer der EU zum Schutz von Geschäftsgeheimnissen höchst unterschiedlich ausgestaltet waren. Die Kommission strebte deshalb einen einheitlichen Schutz an. Ein entsprechender Richtlinienentwurf „über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung“ 2013/0402 (COD) wurde erstmals von der Kommission am 28.11.2013 vorgestellt. Am 14. April 2016 wurde die sog. Know-how Richtlinie vom Europäischen Parlament verabschiedet. Die einzelnen Mitgliedsstaaten müssen diese nunmehr bis 2018 in nationales Recht umsetzen.

Neue Definition des Geschäftsgeheimnisses

Auch für Deutschland bringt die Umsetzung einige bedeutende Veränderungen mit sich. Hier ist insbesondere die Einführung einer neuen Definition des Geschäftsgeheimnisses zu nennen, die sich im Wesentlichen an Art. 39 Abs. 2 des sog. TRIPS-

Übereinkommens („Agreement on Trade-Related Aspects of Intellectual Property Rights“) orientiert. Geschäftsgeheimnisse sind danach künftig nur solche Informationen, die (i) geheim sind, (ii) einen kommerziellen Wert haben und (iii) Gegenstand von angemessenen Geheimhaltungsmaßnahmen sind (vgl. Art. 2 Nr. 1 der Richtlinie). Von besonderer Bedeutung ist dabei das dritte Kriterium der angemessenen Geheimhaltungsmaßnahmen, da damit die Begriffsbestimmung der Richtlinie von dem bisher in Deutschland geltenden Begriffsverständnis deutlich abweicht. Bislang reichte für die Schutzfähigkeit einer Information nach dem UWG ein erkennbarer subjektiver Geheimhaltungswille, der sich in objektiven Umständen manifestiert und immer dann vermutet wurde, wenn es sich um nicht-offenkundige Betriebsinterna handelte. Dies führte letztlich prozessual zu einer Beweislastumkehr. Nunmehr erlangt jedoch nur derjenige Know-how Schutz, der entsprechende Geheimhaltungsmaßnahmen getroffen hat und diese (in einem Verletzungsverfahren) durch eine ordnungsgemäße Dokumentation auch nachweisen kann. Dabei lässt die Richtlinie allerdings ebenso wie Art. 39 des TRIPS-Abkommens die Frage offen, in welchen Fällen von „angemessenen Schutzmaßnahmen“ auszugehen ist.

Reverse Engineering – nun also doch!

Darüber hinaus lässt die Richtlinie zukünftig das in Deutschland bislang verbotene sogenannte „Reverse Engineering“ zu. Reverse Engineering bezeichnet den Nachbau von Produkten durch die tiefe Analyse der konkreten Vorlage. Dies ergibt sich aus dem Erwägungsgrund 10 der Know-how Richtlinie, wodurch Innovation und Wettbewerb gefördert werden sollen. Zwar lässt die Richtlinie die Vereinbarung vertraglicher Beschränkungen hinsichtlich der Nutzung von Geschäftsgeheimnissen zumindest im Verhältnis zu Geschäftspartnern zu. Jedoch sind Dritte an einer solchen Analyse nicht gehindert.

Mitarbeiter – ein Risikofaktor?

Schließlich betreffen die Änderungen im Bereich Geheimnisschutz insbesondere auch das Verhältnis zu den eigenen Mitarbeitern, denn vornehmlich sind sie es, die mit betriebsinternen und innovativen Vorgängen befasst sind und damit zwangsläufig mit Geschäftsgeheimnissen in Berührung kommen. Folglich entsteht die größte Gefahr der Know-how Nutzung durch Dritte wohl dann, wenn diese einen ehemaligen Mitarbeiter des eigenen Unternehmens anstellen und die ehemaligen Mitarbeiter schützenswerte Informationen weitergeben. Die Richtlinie jedenfalls steht der Nutzung von Erfahrungen, die ein Arbeitnehmer im Verlauf seiner Tätigkeit erworben hat, nicht entgegen.

Unser Kommentar

Vor dem Hintergrund der nunmehr verabschiedeten Richtlinie sollte ein geeignetes Schutzkonzept entwickelt und etabliert werden, das dem neuen Begriffsverständnis der Geschäftsinformationen gerecht wird. Im Falle eines eingeleiteten Verletzungsverfahrens muss nämlich insbesondere nachgewiesen werden können, dass die betroffenen geheimen Informationen auch Gegenstand „angemessener Geheimhaltungsmaßnahmen“ in Form eines Schutzkonzepts waren. Mit der Entwicklung und Umsetzung eines entsprechenden Schutzkonzepts sollte nicht bis zur Umsetzung der Richtlinie in nationales Recht gewartet werden. Es besteht nämlich die Möglichkeit, dass Gerichte das deutsche Recht bereits zuvor im Lichte der Richtlinie auslegen und einen Schutz geschäftlicher Informationen nur unter verschärften Anforderungen anerkennen werden. Noch unklar ist, ob die Vorschriften des UWG zum Geheimnisschutz durch die Umsetzung der Know-how-Richtlinie entfallen oder aufgrund des strafrechtlichen Charakters des § 17 UWG weiterhin zur Anwendung kommen werden.

Die künstlerische Gestaltung kann einen Eingriff in Urheber- und Leistungsschutzrechte rechtfertigen

BVerfG, Urt. v. 31. Mai 2016, Az.: 1 BvR 1585/13

Auf den Punkt.

Das Bundesverfassungsgericht („BVerfG“) hat entschieden, dass sich Musikschaffende bei der Übernahme von Ausschnitten aus fremden Tonträgern (sogenannte Sampler) auf die Kunstfreiheit berufen und die Verwertungsinteressen des Tonträgerherstellers zugunsten der künstlerischen Gestaltung zurücktreten können, wenn die Verwertungsmöglichkeit nur geringfügig beschränkt wird. Bislang hatte der Bundesgerichtshof („BGH“) für eine Anwendung des § 24 Abs. 1 UrhG, wonach ein selbständiges Werk, das in freier Benutzung des Werkes eines anderen geschaffen worden ist, ohne Zustimmung des Urhebers des benutzten Werkes veröffentlicht und verwertet werden darf, das zusätzliche Kriterium der fehlenden gleichwertigen Nachspielbarkeit des übernommenen Ausschnitts gefordert.

Hintergrund

Der BGH hatte mit Urteil vom 13. Dezember 2012 (Az.: I ZR 182/11) in Fortführung seiner Rechtsprechung vom 20. November 2008 (Az.: I ZR 112/06) entschieden, dass die Übernahme einer 2-sekündigen Sequenz aus der Tonspur des Musikwerkes „Metall auf Metall“ der Band Kraftwerk in den Titel „Nur mir“ in Form des sogenannten Samplings einen Eingriff in das Tonträgerrecht darstelle. Dieser Eingriff sei nicht durch das Recht auf freie Benutzung gemäß § 24 Abs. 1 UrhG gedeckt, da die Übernahme einer fremden Sequenz, und sei sie auch noch so kurz, nur übernommen werden dürfe, wenn sie nicht gleichwertig nachgespielt werden könne. Gegen dieses Urteil hatten die Beschwerdeführer Verfassungsbeschwerde beim BVerfG eingelegt.

Die Entscheidung

Das BVerfG hat das Urteil des BGH wegen Verletzung der Beschwerdeführer in ihrer gem. Art. 5 Abs. 3 Satz 1 GG gewährleisteten Kunstfreiheit aufgehoben und zur erneuten Entscheidung an den BGH zurückverwiesen. Zur Begründung führte das Gericht aus, dass bei der Auslegung und Anwendung des Urheberrechts eine Interessenabwägung zwischen dem Verwertungsinteresse des Tonträgerherstellers und der gegenüberstehenden Grundrechtsposition vorzunehmen sei. Die Entscheidung des BGH, wonach die Übernahme selbst kleinster Tonsequenzen einen unzulässigen Eingriff darstelle, soweit diese gleichwertig nachspielbar seien, trage der Kunstfreiheit nicht in ausreichendem Maße Rechnung und stelle eine zu enge Auslegung des Begriffes der „freien Benutzung“ nach § 24 UrhG dar. Der Verweis auf eine bestehende Lizenzierungsmöglichkeit ändere nichts daran, da kein Anspruch auf die Einräumung einer Lizenz bestehe; der Tonträgerhersteller könne eine solche verweigern oder von der Zahlung einer unverhältnismäßig hohen Lizenzgebühr abhängig machen. Ebenso wenig stelle das eigene Nachspielen von Klangfolgen einen gleichwertigen Ersatz für das Sampeln dar. Es handele sich beim Sampeln nämlich um eine eigene Stilprägung, die als Element dem Hip-Hop immanent sei. Zudem könne sich das Nachstellen von Tonsequenzen als sehr aufwendig darstellen.

Darüber hinaus stelle die erlaubnisfreie Zulässigkeit des Samples nur einen geringfügigen Eingriff in das Tonträgerrecht dar. Es sei nicht ersichtlich, dass aufgrund der Sequenzübernahme die Gefahr des Absatzrückgangs drohe. Dies läge nur dann nahe, wenn das neue Werk eine große Nähe zu dem Originalwerk aufweise und davon auszugehen sei, dass dieses bestimmungsgemäß in Konkurrenz zu dem ursprünglichen Werk treten werde. Relevante Kriterien seien insbesondere die künstlerische aber auch zeitliche Nähe zum Ursprungswerk, die Bedeutung und Bekanntheit des übernommenen Abschnitts sowie die wirtschaftliche Signifikanz eines drohenden Schadens für den Urheber des Originalwerks. Der Grund dafür, dem Tonträgerhersteller ein Schutzrecht zu gewähren, sei auch nicht, ihm Lizenzeinnahmen zu sichern, sondern ihn vor der Gefährdung seines wirtschaftlichen Einsatzes zu schützen. Infolgedessen sei der Schutz kleiner und kleinster Teile von Verfassung wegen nicht geboten, wenn

dadurch die Nutzung des kulturellen Bestands erschwert oder gar unmöglich gemacht werde.

Unser Kommentar

Durch seine Entscheidung hat sich das BVerfG von der bisherigen Rechtsprechung des BGH distanziert und den Stellenwert der Kunstfreiheit deutlich angehoben. Interessant wird sein, wie der BGH die Bedeutung des Art. 5 Abs. 3 Satz 1 GG in seine erneute Entscheidung einfließen lassen wird. Denn das BVerfG hat offengelassen, ob die Berücksichtigung der Kunstfreiheit etwa in Form einer entsprechenden Anwendung von § 24 Abs. 1 UrhG oder durch eine begrenzende Auslegung von § 85 Abs. 1 Satz 1 UrhG, wonach der Hersteller eines Tonträgers das ausschließliche Recht hat, den Tonträger zu vervielfältigen, zu verbreiten und öffentlich zugänglich zu machen, erfolgen sollte. Das BVerfG wies aber darauf hin, dass der BGH u.U. verpflichtet sein könne, den Fall dem EuGH zur Vorabentscheidung über die Auslegung der zugrundeliegenden EU-rechtlichen Vorgaben vorzulegen.

„Internetpranger"

OLG München, Urt. v. 17. März 2016, Az.: 29 U 368/16

Auf den Punkt.
Die Veröffentlichung eines Profilbildes aus einem sozialen Netzwerk in einer Berichterstattung über fremdenfeindliche Äußerungen im Rahmen der Flüchtlingsdebatte ist rechtswidrig.

Der Fall

Eine Zeitung hatte im Oktober 2015 Kommentare von Facebook-Nutzern, in denen diese gegen Flüchtlinge hetzten, mit Profilbild, Namen und dem geposteten Text abgebildet. Die Zeitung kommentierte den dargestellten Text wie folgt:

> *„(…) Hass auf Flüchtlinge: (...) stellt die Hetzer an den Pranger: Deutschland ist entsetzt: Ganz offen und mit vollem Namen wird in sozialen Netzwerken zu Gewalt aufgerufen und gehetzt – gegen Ausländer, Politiker, Journalisten, Künstler ... (…). Längst ist die Grenze überschritten von freier Meinungsäußerung oder Satire zum Aufruf zu schwersten Straftaten bis zum Mord. (...). Wir stellen die Hetzer an den Pranger! Herr Staatsanwalt, übernehmen Sie!"*

Eine Betroffene, die mit ihrem Beitrag, Namen und Profilbild abgebildet war, ging gegen die Abbildung ihres Bildes im Wege des einstweiligen Verfügungsverfahrens vor. Mit ihrem Antrag wollte sie die Veröffentlichung ihres Profilbildes verbieten lassen. Mit Urteil vom 10. Dezember 2015 hatte das Landgericht München I den Verfügungsantrag der Antragstellerin zurückgewiesen. Nach Auffassung des Landgerichts lag keine rechtswidrige Verletzung des Persönlichkeitsrechts der Antragstellerin vor. Hiergegen legte die Antragstellerin Berufung ein.

Die Entscheidung

Die Berufung hat Erfolg. Der Antragstellerin steht gegenüber der Antragsgegnerin der geltend gemachte Unterlassungsanspruch nach §§ 823 Abs. 1, 1004 BGB, 22

KUG, Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG wegen der Verwendung ihres Bildes zu. Nach Ansicht des OLG München ist die streitgegenständliche Bildveröffentlichung unzulässig.

Das OLG München stellte zunächst fest, dass die Antragstellerin auf dem wiedergegebenen Profilbild erkennbar sei und die Abbildung daher ein Bildnis im Sinne der § 22, 23 KUG sei. Hinzu komme, dass neben der Abbildung auch der Name der Antragstellerin mitgeteilt werde. Angesichts der Verbindung von Namensangabe und Bild stehe die Identifizierbarkeit der Antragstellerin außer Zweifel. Nach Auffassung des OLG München habe die Antragstellerin weder, wie nach § 22 KUG erforderlich, ausdrücklich noch konkludent in die Veröffentlichung des Bildes eingewilligt. Eine Einwilligung ergebe sich insbesondere nicht aus dem Umstand, dass die Antragstellerin das streitgegenständliche Foto selbst in ein soziales Netzwerk eingestellt habe, ohne von möglichen Zugriffssperren Gebrauch zu machen. Nach Ansicht des Gerichtes willige ein Nutzer allein durch das Einstellen einer Fotografie auf seinen Account bei einem sozialen Netzwerk weder ausdrücklich noch stillschweigend in die Weiterverbreitung des Fotos durch Dritte außerhalb des Kreises der zugriffsberechtigten Mitglieder des Netzwerkes im Rahmen eines gänzlich anderen Kontexts ein. Ebenso ergebe sich auch keine Zulässigkeit aus § 23 Abs. 1 Nr. 1 KUG. Hiernach dürfen Bildnisse aus dem Bereich der Zeitgeschichte zwar ohne die nach § 22 KUG erforderliche Einwilligung verbreitet werden. Dies erfordere jedoch eine Abwägung der widerstreitenden Interessen. Unter Berücksichtigung dieser Abwägung verstoße die Abbildung des Profilbildes nach Ansicht des OLG Münchens gegen das Persönlichkeitsrecht der Antragstellerin.

Entgegen der Rechtsansicht der Antragsgegnerin stehe dieser Einschätzung auch nicht das Informationsinteresse der Öffentlichkeit entgegen. Nach Ansicht des Gerichtes habe die Zeitung kein berechtigtes Interesse daran, die Antragstellerin im Rahmen der Wiedergabe ihrer Äußerung durch die Abbildung eines mit ihrem Namen versehenden Fotos kenntlich zu machen. Insbesondere sei nicht erkennbar, welche Bedeutung es für eine sachbezogene Erörterung der in der Flüchtlingsdebatte in einem Interneteintrag geäußerten Meinung einer beliebigen Person aus Sicht des angesprochenen Publikums haben könnte, zu wissen, wie diese Person heißt und aussieht. Zur Darstellung des Meinungsbilds und dessen Bewertung bedürfe es lediglich der Mitteilung der Äußerung der Antragstellerin. Das Bildnis einer Person werde nicht schon dadurch zu einem Bildnis der Zeitgeschichte, dass sich die fragliche Person in einem Interneteintrag zum Zeitgeschehen geäußert habe. Das Recht des Abgebildeten überwiege regelmäßig das Recht der Presse, wenn eine sachbezogene Berichterstattung auch durch Wiedergabe der Äußerung des Abgebildeten möglich sei.

Unser Kommentar

Das vorliegende Urteil beschäftigt sich mit der Frage, ob eine Veröffentlichung eines bei Facebook eingestellten Profilbildes zulässig ist und insbesondere mit der Problematik, ob das bloße Einstellen eines Fotos in ein soziales Netzwerk eine Einwilligung zur Nutzung durch Dritte darstellt. Diese Thematik wird gerade in jüngster Zeit durch die weit verbreitete Nutzung von sozialen Netzwerken und die damit einhergehende Öffnung der Privatsphäre durch Veröffentlichung von Bildern relevant. Zu Recht verneint das OLG München im vorliegenden Fall jedoch eine Einwilligung, da diese voraussetzt, dass der Einwilligende Zweck, Art und Umfang der geplanten Verwendung kennt. Dies war vorliegend nicht der Fall. Auch rechtfertigt im vorliegenden Fall das Informationsinteresse nicht die Abbildung von Fotos. Anders als beispielsweise die Abbildung einer Person, die im Rahmen einer öffentlichen Demonstration ihre Meinung auf einem Plakat darstellt, wird im vorliegenden Fall eine sachliche Auseinandersetzung mit der Flüchtlingsdebatte auch ohne Abbildung der Personen ermöglicht. Zusammenfassend lässt sich somit festhalten, dass, je nach Informationsinteresse der Allgemeinheit, die Veröffentlichung von Kommentaren aus sozialen Netzwerken durchaus zulässig sein kann, die konkrete Darstellung jedoch Frage des Einzelfalls sein wird.

Arbeitgeber darf Browserdaten von Arbeitnehmer-PC auswerten

LAG Berlin-Brandenburg, Urt. v. 14. Januar 2016, Az.: 5 Sa 657/15

Auf den Punkt.

Die unerlaubte Privatnutzung des Internets am Arbeitsplatz stellt nach gefestigter arbeitsgerichtlicher Rechtsprechung eine Arbeitspflichtverletzung dar. Nach wie vor besteht zwar Klärungsbedarf, wie der Beweis der Privatnutzung vor dem Hintergrund des Verfassungs- und Datenschutzrechts geführt werden kann. Das Urteil des Landesarbeitsgerichts („LAG") Berlin-Brandenburg stellt jedoch klar, dass unter bestimmten Voraussetzungen der Browserverlauf des Dienstrechners des Arbeitnehmers auch ohne dessen Einwilligung zu Beweiszwecken verwertet werden kann. Ein Beweisverwertungsverbot besteht nicht, wenn dem Arbeitgeber keine anderen Mittel zum Beweis des Missbrauchs des dienstlichen Internetanschlusses zur Verfügung steht.

Der Fall

Der Kläger ist seit 1998 als „Gruppenleiter Konstruktion" bei der Beklagten beschäftigt, wobei er seine Tätigkeit in einem Einzelbüro mit Dienstrechner ausführt. Der Arbeitsvertrag des Klägers sieht stichprobenartige Kontrollen der Internetnutzung durch die Beklagte vor. Aufgrund des sehr hohen Datenvolumens des Unternehmens wurde kontrolliert, wer dieses Datenvolumen verursacht. Bei der Kontrolle wurde festgestellt, dass der Dienstrechner des Klägers ein Datenvolumen in einem Umfang aufweist, wie dies sonst nur bei Servern der Beklagten vorkomme. Die Beklagte befragte den Kläger, ob er den Dienstrechner auch privat nutze, welches der Kläger bejahte. Zudem räumte der Kläger ein, jederzeit mit einer Abmahnung gerechnet zu haben. Die Beklagte hörte anschließend den Betriebsrat an und kündigte das Arbeitsverhältnis daraufhin außerordentlich fristlos. Der IT-Leiter überprüfte den Dienstrechner des Beklagten im Beisein zweier Betriebsratsmitglieder und nahm Einsicht in die Browserdaten. Es wurde festgestellt, dass in einem Zeitraum von 30 Arbeitstagen bei einer täglichen Arbeitszeit von 8 Stunden 16.369 private Seitenaufrufe stattfanden. Bei den Seitenaufrufen handelt es sich größtenteils um online Marktplätze, Internetseiten mit pornographischem Inhalt sowie Seiten, die den illegalen Download von Musik- und Filmwerken ermöglichen. Der Kläger behauptet, dass die private Internetnutzung auf den Dienstrechnern des Arbeitgebers nicht verboten sei und auch seine Kollegen den Internetanschluss des Arbeitgebers für private Zwecke verwenden. Die Beklagte berief sich dagegen auf die IT-Nutzerrichtlinie, die die Privatnutzung des Internets ohne Ausnahme untersage.

Die Entscheidung

Der Kläger begehrte im Wege der Kündigungsschutzklage die Feststellung der Unwirksamkeit der außerordentlichen Kündigung und zusätzlich eine Annahmeverzugsvergütung, die Weiterbeschäftigung, Schadensersatz und Schmerzensgeld.

Die Klage hatte keinen Erfolg. Zur Begründung führte das LAG aus, in der exzessiven privaten Nutzung des dienstlichen Internetanschlusses durch den Kläger liege ein wichtiger Grund im Sinne des § 626 Abs. 1 BGB, der zur außerordentlichen Kündigung berechtige. Die festgestellten Seitenaufrufe entsprachen unter Annahme, dass jeder Seitenaufruf nur wenige Sekunden in Anspruch nahm, mindestens 39,86 Stunden in einem Zeitraum von 30 Arbeitstagen. Bei einer wöchentlichen Arbeitszeit von 40 Stunden und unter Berücksichtigung der Ruhepausen entspreche diese Zeit etwa drei Arbeitstagen, an denen der Kläger seiner Arbeitspflicht nicht nachgekommen sei. Eine derartige Vernachlässigung der Arbeitspflicht stelle eine schwere Pflichtverletzung und im Einzelfall einen wichtigen Grund dar. Aufgrund der Schwere der Pflichtverletzung sei die Beklagte auch unter Berücksichtigung der bereits 16-jährigen Betriebszugehörigkeit des Klägers nicht verpflichtet gewesen, den Kläger zunächst abzumahnen.

Das Gericht verneinte auch das Vorliegen eines Beweisverwertungsverbots. Die Zivilprozessordnung kenne für rechtswidrig erlangte Informationen kein allgemeines Verwertungsverbot. Vielmehr ergebe sich aus § 286 ZPO i.V.m. Art. 103 Abs. 1 GG die Verpflichtung der Gerichte, angebotene Beweise auch zu berücksichtigen. Der Richter sei aber zugleich an die Grundrechte gebunden und zu einer rechtsstaatlichen Verfahrensführung verpflichtet, weshalb jeweils zu prüfen sei, ob die Beweiserhebung und -verarbeitung auf eine

gesetzliche Grundlage gestützt werden könne und das Vorgehen im Übrigen mit dem allgemeinen Persönlichkeitsrecht des Betroffenen zu vereinbaren sei. Das Gericht ging davon aus, dass es sich bei den Browserdaten um personenbezogene Daten im Sinne des Bundesdatenschutzgesetztes („BDSG“) handle und dass die Erhebung und Verarbeitung dieser Daten auch ohne Einwilligung des Klägers gem. § 32 Abs. 1 S. 1 BDSG erlaubt sei. Danach können personenbezogene Daten zu Zwecken des Beschäftigungsverhältnisses erhoben, verarbeitet und genutzt werden, wenn dies für die Entscheidung über dessen Begründung, oder dessen Durchführung oder Beendigung erforderlich ist. Dies sei vorliegend der Fall; die Beklagte habe ein legitimes Interesse, Einsicht in den Browserverlauf zu nehmen, um eine missbräuchliche Nutzung des Internetzugangs festzustellen. Die Auswertung sei auch erforderlich gewesen, da die konkrete Art des Missbrauchs ausschließlich durch die Auswertung der Browserverlaufsdaten erfolgen konnte. Auch sei die Anwesenheit des Klägers bei der Einsichtnahme kein milderes Mittel gewesen, da sich weder die Art des Abrufs noch die letztendliche Feststellung des Verstoßes dadurch geändert hätten.

Unser Kommentar

Das Urteil des LAG Berlin-Brandenburg hilft Arbeitgebern (vorläufig) in der Beurteilung, unter welchen Voraussetzungen die Auswertung des Browserverlaufs des Dienstrechners eines Arbeitnehmers bei dem Verdacht auf eine unzulässige private Internetnutzung, vorgenommen werden dürfen. Dies ist begrüßenswert, da in diesem Bereich noch sehr viel Rechtsunsicherheit herrscht. Grundsätzlich ist es empfehlenswert, im Arbeitsvertrag, einer Betriebsvereinbarung oder IT-Richtlinie eindeutige Regelungen zur (Un-) Zulässigkeit der privaten Nutzung der Unternehmens-IT zu treffen und die Einhaltung der Regelungen regelmäßig zu kontrollieren. Klare Regeln erhöhen die Möglichkeiten des Arbeitgebers im Einzelfall auch belastbare Beweise zu erlangen.

Das Urteil des LAG Berlin-Brandenburg ist noch nicht rechtskräftig; die Revision ist anhängig unter dem Aktenzeichen: 2 AZR 198/16.

Unzulässigkeit von Werbung in Bestätigungs-E-Mails

BGH, Urt. v. 15. Dezember 2015,
Az.: VI ZR 134/15

Auf den Punkt.
Automatisch generierte Antwort-Emails dürfen keine Werbung enthalten, wenn der adressierte Verbraucher dem widersprochen hat. Im Falle eines (auch geringfügigen) Verstoßes kann dies einen Unterlassungsanspruch begründen. Zudem drohen Bußgelder in Höhe von bis zu 250.000 Euro.

Der Fall

Gegenstand der vorliegenden Entscheidung war die Klage eines Verbrauchers gegen eine Versicherung. Der Kläger wandte sich mit der Bitte um Bestätigung einer von ihm ausgesprochenen Kündigung per E-Mail an die Beklagte. Die Beklagte bestätigte unter dem Betreff “Automatische Antwort auf Ihre Mail (...)” den Eingang der klägerischen E-Mail. Diese Eingangsbestätigung enthielt am Ende folgende zwei Hinweise auf einen SMS-Service und eine App für Unwetterwarnungen der Beklagten:

> *„Übrigens: Unwetterwarnungen per SMS kostenlos auf Ihr Handy. Ein exklusiver Service nur für S. Kunden. Infos und Anmeldung unter (…)*
>
> *Neu für iPhone Nutzer: Die App S. Haus & Wetter, inkl. Push Benachrichtigungen für Unwetter und vielen weiteren nützlichen Features rund um Wetter und Wohnen: (…)“*

Daraufhin wandte sich der Kläger erneut per E-Mail an die Beklagte und rügte, dass die automatisierte Antwort-E-Mail Werbung enthalte, mit der er nicht einverstanden sei. Auch auf diese zweite E-Mail sowie eine weitere mit einer Sachstandsanfrage erhielt der Kläger automatisierte Empfangsbestätigungen mit denselben Hinweisen. Mit der Klage begehrte der

Kläger von der Beklagten, es zu unterlassen, ihn ohne sein Einverständnis zu Werbezwecken per E-Mail zu kontaktieren.

Das Amtsgericht hatte zunächst der Klage stattgegeben. Auf die Berufung der Beklagten änderte das Landgericht das Urteil des Amtsgerichts ab und wies die Klage ab. Mit der vom Landgericht zugelassenen Revision begehrte der Kläger Wiederherstellung des erstinstanzlichen Urteils.

Die Entscheidung

Die Revision des Klägers hatte Erfolg. Der BGH entschied, dem Kläger stehe ein Anspruch auf Unterlassung aus §§ 823 Abs. 1, 1004 Abs. 1 Satz 2 BGB gegen die Beklagte wegen eines rechtswidrigen Eingriffs in sein allgemeines Persönlichkeitsrecht zu. Auch Autoreply-E-Mails mit werblichem Inhalt seien nämlich unzulässig, wenn der Verbraucher dem Erhalt von E-Mail-Werbung widersprochen hat. Der Begriff der Werbung sei weit zu verstehen; Werbung erfasse jede Äußerung bei der Ausübung eines Handels, Gewerbes, Handwerks oder freien Berufs mit dem Ziel, den Absatz von Waren oder die Erbringung von Dienstleistungen zu fördern. Mit den Hinweisen auf die kostenlosen Unwetterwarnungen per SMS oder App bewerbe die Beklagte ihre Produkte. Dass die Werbung in eine automatisch generierte Eingangsbestätigung eingebunden gewesen sei, rechtfertige keine andere Beurteilung.

Differenziert werden müsse aber grundsätzlich, ab wann ein Eingriff in das allgemeine Persönlichkeitsrecht vorliegt. Das allgemeine Persönlichkeitsrecht schütze den Bereich privater Lebensgestaltung und gebe dem Betroffenen das Recht, im privaten Bereich in Ruhe gelassen zu werden. Daher könne das allgemeine Persönlichkeitsrecht vor Belästigungen schützen, die von einer unerwünschten Kontaktaufnahme ausgehen. In der bloßen Kontaktaufnahme könne aber regelmäßig nur dann eine Belästigung liegen, wenn sie gegen den eindeutig erklärten Willen des Betroffenen erfolgt. Entscheidend sei vorliegend, dass der Empfänger diese Art der Werbung ausdrücklich abgelehnt habe, sich praktisch aber nicht gegen das unerwünschte Eindringen der Werbung zur Wehr setzen konnte. Insbesondere weil die Werbung an den erwarteten Inhalt einer Antwort der Beklagten angehängt gewesen sei, die zudem zu Beweiszwecken relevant sein könnte, habe der Adressat keine Chance gehabt, sich der Werbung beispielsweise über einen Spam-Filter zu entziehen. Aus dem Umstand, dass der Kläger die Kommunikation begonnen hatte, folgte kein Einverständnis in den Erhalt von Werbung.

In dem vorliegenden Fall konnte sich der BGH allerdings darauf beschränken festzustellen, dass jedenfalls die dritte Bestätigungs-E-Mail mit werblichem Inhalt gegen den eindeutig erklärten Willen des Klägers erfolgte. Ob jedoch bereits die zweite oder sogar die erste automatische Antwort-E-Mail unzulässig waren, ließ der BGH offen.

Unser Kommentar

Die Entscheidung des BGH überrascht nicht, wenn man bedenkt, dass für reine E-Mail-Werbung in der Regel die ausdrückliche Einwilligung des Betroffenen eingeholt werden muss, beweissicher über das sog. Double-Opt-In-Verfahren. Daher sollte auch der Versand von Bestätigungs-E-Mails mit Werbeinhalten (bereits beim erstmaligen Versand) nur dann erfolgen, wenn eine vorherige Einwilligung des Empfängers nachweisbar eingeholt worden ist. Zudem erscheint fraglich, ob sich in der Praxis ein Mechanismus umsetzen lässt, wonach sichergestellt ist, dass zumindest nach Eingang eines Widerspruchs automatisch generierte E-Mails nur noch ohne werbende Inhalte versandt werden. Unternehmen ist daher zu raten, in Autoreply-E-Mails auf Werbung zu verzichten.

Veranstaltungen

Termin	Thema/Referent	Veranstalter/Ort
28. - 29. Juli 2016	**Crashkurs IT-Recht** *(Dr. Michael Rath, Christian Kuß, LL.M., Simone Bach, LL.M., Christoph Maiworm, Michael Wiedemann, SAP SE)*	Management Circle AG München
06. September 2016	**Aktuelle Entwicklungen im Datenschutz** EBZ-Seminar *(Silvia C. Bauer)*	Europäisches Bildungszentrum der Wohnungs- und Immobilienwirtschaft Frankfurt
27. September 2016	**Urheber- und Designrecht** IHK Ruhr - Veranstaltungsreihe "Idee trifft Recht" *(Dr. Maximilian Dorndorf)*	IHK Ruhr Essen
28. September 2016	**Terrorscreening – Mögliche Risiken für Immobilienunternehmen** EBZ-Seminar *(Silvia C. Bauer)*	Europäisches Bildungszentrum der Wohnungs- und Immobilienwirtschaft Online (Webinar)
06. - 07. Oktober 2016	**Rechtsfragen Social Media-Marketing** *(Christian Kuß, LL.M.)*	Management Circle AG Frankfurt
02. - 03. November 2016	**Der erfolgreiche Digital Manager** *(Christoph Maiworm)*	Management Circle AG Frankfurt
09. November 2016	**Aktuelle Entwicklungen im Datenschutz** EBZ-Seminar *(Silvia C. Bauer)*	Europäisches Bildungszentrum der Wohnungs- und Immobilienwirtschaft Bochum

Weitere Informationen zu den Veranstaltungen der Luther Rechtsanwaltsgesellschaft mbH finden Sie auf unserer Homepage unter dem Stichwort „Veranstaltungen“.

Impressum

Verleger: Luther Rechtsanwaltsgesellschaft mbH
Anna-Schneider-Steig 22, 50678 Köln, Telefon +49 221 9937 0
Telefax +49 221 9937 110, contact@luther-lawfirm.com
V.i.S.d.P.: Dr. Michael Rath, Partner
Luther Rechtsanwaltsgesellschaft mbH, Anna-Schneider-Steig 22
50678 Köln, Telefon +49 221 9937 25795
michael.rath@luther-lawfirm.com

Die Luther Rechtsanwaltsgesellschaft mbH berät in allen Bereichen des Wirtschaftsrechts. Zu den Mandanten zählen mittelständische und große Unternehmen sowie die öffentliche Hand.

Berlin, Brüssel, Düsseldorf, Essen, Frankfurt a. M., Hamburg, Hannover, Köln, Leipzig,
London, Luxemburg, München, Shanghai, Singapur, Stuttgart, Yangon

Luther Corporate Services: Delhi-Gurgaon, Kuala Lumpur, Shanghai, Singapur, Yangon

Ihren Ansprechpartner finden Sie auf www.luther-lawfirm.com

Auf den Punkt. Luther.

JUVE AWARDS 2014 Kanzlei des Jahres für Regulierte Industrien

JUVE AWARDS 2014 Kanzlei des Jahres für Energiewirtschaftsrecht

JUVE AWARDS 2014 Kanzlei des Jahres für Privates Baurecht

JUVE AWARDS 2015 Kanzlei des Jahres für Vertrieb/Handel/Logistik