Luther.

IP/IT

(Intellectual Property/Information Technology)

Das neue deutsche Datenschutzrecht

Die Medienanstalt Hamburg / Schleswig-Holstein geht gegen Schleichwerbung auf YouTube vor

Drittinhalte auf Webseiten in Gefahr: Gefällt Facebooks „Gefällt mir“ den Gerichten?

Zum Zu-Eigen-Machen von Äußerungen durch den Betreiber eines Bewertungsportals

Bösgläubigkeit einer Markenanmeldung

Weitere Themen im Innenteil

Newsletter 2. Ausgabe 2017

Das neue deutsche Datenschutzrecht

Auf den Punkt.

Die Datenschutz-Grundverordnung (DSGVO) wird das in Deutschland geltende Datenschutzrecht verändern. Die DSGVO soll das Datenschutzrecht in den Mitgliedstaaten vereinheitlichen; gleichwohl darf der nationale Gesetzgeber eigene Regelungen treffen. Hierzu hat der Bundestag am 27. April 2017 das Gesetz zur Anpassung des Datenschutzrechts an die DSGVO und zur Umsetzung der Richtlinie (EU) 2016/680 (DSAnpUG) beschlossen.

Hintergrund

Die DSGVO wird ab dem 25. Mai 2018 in jedem EU-Mitgliedsland geltendes Recht sein (siehe http://www.luther-lawfirm.com/publikationen/newsletter/inhalt/sondernewsletter-ipit-1-2016.html#i2046). Als Verordnung wirkt sie unmittelbar und muss nicht mehr in nationales Recht umgesetzt werden. Gleichwohl sieht die DSGVO an vielen Stellen sog. Öffnungsklauseln vor, die den Mitgliedstaaten Gestaltungsspielräume für eigene nationale Regelungen ermöglichen. Abhängig von dem jeweiligen Regelungskontext können die Mitgliedstaaten Regelungen der DSGVO bei Vorliegen einer Öffnungsklausel ersetzen, ergänzen oder näher konkretisieren.

Die Regelungen

Zunächst fällt auf, dass das BDSG-neu allein durch die Anzahl der 85 Paragraphen für ein bloßes Anpassungs- und Umsetzungsgesetz eine sehr umfangreiche Regelung darstellt. Gegenüber der Anzahl der Paragraphen des derzeitigen Bundesdatenschutzgesetzes (BDSG) sind noch einmal fast die Hälfte an Paragraphen dazu gekommen. Im Folgen sollen die für das wirtschaftliche Umfeld wichtigsten Neuerungen vorgestellt werden.

1. Beschäftigtendatenschutz

§ 26 BDSG-neu soll die Datenverarbeitung im Beschäftigungsverhältnis aufgrund der Öffnungsklausel des Art. 88 DSGVO regeln. Dafür werden zunächst im Wortlaut größtenteils die derzeitigen deutschen Regelungen zum Beschäftigtendatenschutz wiedergegeben. Ausdrücklich neu aufgenommen wurde, dass Daten von Beschäftigten verarbeitet werden dürfen, sofern dies zur „Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag oder einer Betriebs- oder Dienstverarbeitung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist“. Kollektivvereinbarungen bleiben also ein zulässiges Mittel, um eine Datenverarbeitung zu erlauben. Sie müssen nun aber die Voraussetzungen von Art. 88 Abs. 2 DSGVO und § 26 BDSG-neu erfüllen. Diese beiden Bestimmungen gelten auch für die Datenverarbeitung durch Betriebsräte. Auch auf die Freiwilligkeit der Einwilligung eines Beschäftigten wird ausdrücklich Bezug genommen. Diese kann insbesondere vorliegen, wenn der Beschäftigte einen wirtschaftlichen Vorteil wählt (private Nutzung von betrieblichen IT-Geräten etc.). Als formelle Voraussetzung wird dabei grundsätzlich verlangt, dass das Einverständnis zur Datenverarbeitung im Beschäftigungsverhältnis unterschrieben vorliegen müsse.

2. Schmerzensgeld

Außerdem können Verbraucher und damit auch Beschäftigte nun auch eine angemessene Geldentschädigung wegen eines durch eine Verarbeitung ihrer personenbezogenen Daten entstandenen Schadens verlangen (§ 83 Abs. 2 BDSG-neu), der kein Vermögensschäden ist. Im Hinblick auf die neuen Verbandsklagerechte, die Verbrauchern und Verbänden bei der Durchsetzung solcher Ansprüche helfen, kommen auf Unternehmen hier erhebliche Risiken zu.

3. Datenschutzbeauftragter

Das BDSG-neu stärkt die Stellung des Datenschutzbeauftragten im Vergleich zur DSGVO und übernimmt im Wesentlichen die bisherigen Regelungen des BDSG. Ein Datenschutzbeauftragter muss bestellt werden, wenn mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, wenn wegen eines hohen Risikos für die Rechte und Freiheiten der von der Datenverarbeitung Betroffenen eine Datenschutz-Folgenabschätzung notwendig ist oder geschäftsmäßig personenbezogene Daten zum Zweck der (anonymisierten) Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet werden. Außerdem bleibt es bei dem erweiterten Kündigungsschutz für einen Datenschutzbeauftragten. Die DSGVO gibt dagegen nur vor,

dass der Datenschutzbeauftragte nicht „wegen der Erfüllung seiner Aufgaben“ abberufen oder benachteiligt werden darf. Zwar bestehen nur für die Pflicht zu seiner Benennung und für die Wahrung der Geheimhaltung oder Vertraulichkeit Öffnungsklauseln. Diesen Gestaltungsspielraum zur Benennung eines Datenschutzbeauftragten versucht der deutsche Gesetzgeber aber offenbar auszureizen. Dies könnte nicht mehr von einer Öffnungsklausel umfasst sein und damit keinen Bestand haben.

Unser Kommentar

Die vielen Verweise und Wiederholungen sowie das unübersichtliche Zusammenspiel mit der DSGVO führen zu erheblichen Anwendungsschwierigkeiten. Das Ziel der DSGVO, ein einheitliches europäisches Datenschutzniveau herzustellen, wird durch die umfangreichen und komplexen Vorschriften konterkariert. Außerdem könnte das BDSG-neu zumindest in Teilen für unzulässig bzw. unvereinbar mit dem Unionsrecht erklärt werden. Denn die zahlreichen Wiederholungen von Regelungen der DSGVO könnten mit dem Wiederholungsverbot des Europäischen Gerichtshofs unvereinbar sein. Nach der Rechtsprechung des EuGH darf ein Mitgliedstaat durch die Umsetzung einer Verordnung grundsätzlich keine Lage schaffen, in der die unmittelbare Geltung der Verordnung in Zweifel gezogen werden könnte. Hier könnte entscheidend sein, ob die Wiederholungen im BDSG-neu ausnahmsweise zulässig sind, weil sie zu einer einheitlichen Anwendung der Vorschriften der DSGVO beitragen und die nationalen Vorschriften verständlicher machen (vgl. Erwägungsgrund 8 der DSGVO). Jedenfalls dürften die Wiederholungen der Vorschriften der DSGVO in der Praxis zu erheblichen Anwendungs- und Auslegungsproblemen führen, da beide Regelungen stets parallel zu beachten sind und etwaige Unterschiede für den Rechtsanwender nur schwer auszumachen sind.

Trotz der umfangreichen Regelungen wurde das Ziel einer ausreichend differenzierten, bundesgesetzlichen Regelung des Beschäftigtendatenschutzes verpasst. Schon § 32 BDSG galt nur als (provisorischer) erster Schritt zu einem Beschäftigtendatenschutzgesetz. Der aktuelle Koalitionsvertrag sah das Ziel einer bundesgesetzlichen Regelung des Beschäftigtendatenschutzes vor, sofern die DSGVO keine eigene Regelung treffe. Die DSGVO enthält lediglich eine Öffnungsklausel für die Mitgliedstaaten. Auf eine vollständige Regelung des Beschäftigtendatenschutzes muss daher weiter gewartet werden. Keinen Aufschub dagegen verdient die Vorbereitung auf das neue Datenschutzrecht. Denn nach der zu erwartenden Zustimmung des Bundesrats soll das BDSG-neu (bis auf wenige Regelungen) zeitgleich mit der DSGVO am 25. Mai 2018 in Kraft treten.

Die Medienanstalt Hamburg/Schleswig-Holstein geht gegen Schleichwerbung auf YouTube vor

Auf den Punkt.
Wer als sog. Influencer auf Social Media Plattformen wie Youtube, Instagram oder Facebook für sich oder Dritte im redaktionellen Rahmen wirbt, ist verpflichtet, den werblichen Charakter seines Beitrages zu kennzeichnen.

Der Fall

Der bekannte Fitness-YouTuber „Flying Uwe“ präsentierte in der Vergangenheit in seinen Videos Eigenprodukte, ohne dies als Werbung zu kennzeichnen. Das stellt nach der Auffassung der Medienanstalt Hamburg / Schleswig-Holstein (MA HSH) einen Verstoß gegen rundfunkrechtliche Werbebestimmungen dar. Aufgrund zahlreicher vergangener Verstöße hatte die MA HSH Flying Uwe bereits aufgefordert, die entsprechenden Videos sowie die dazugehörigen Videobeschreibungen auf seinem YouTube Kanal als Werbung zu kennzeichnen. Zwar kam er dieser Aufforderung zum Teil nach. Bei solchen Videos, in denen er Produkte seines eigenen Unternehmens präsentierte, fehlten aber auch weiterhin die erforderlichen Werbekennzeichnungen. Vor diesem Hintergrund leitete die MA HSH ein medienrechtliches Verfahren wegen eines Verstoßes gegen die Werbebestimmungen des § 58 Abs. 3 RStV ein.

Hintergrund

Influencer Marketing erfreut sich einer rasant steigenden Beliebtheit bei werbenden Unternehmen. Denn mit den neuen Stars aus dem Internet lässt sich auf relativ einfachem Weg eine hohe Reichweite auf den relevanten Social Media Kanälen erzielen. Influencer binden dabei die Leistungen oder Produkte ihrer Sponsoren geschickt in ihren Beitrag ein, sodass sich die Zielgruppe bestmöglich unterhalten fühlt. Dabei wird jedoch die Grenze zwischen den werblichen und den nicht-werblichen Inhalten nicht immer eingehalten. Dies bringt allerdings Risiken mit sich, für Influencer und für Unternehmen, welche den

Influencer für eine Kampagne gebucht haben. Zum einen kann die zuständige Medienanstalt ein Verfahren wegen eines Verstoßes gegen Werbebestimmungen eröffnen. Außerdem besteht die Gefahr, von Wettbewerbern oder der Wettbewerbszentrale in Anspruch genommen zu werden.

Bei Influencer Beiträgen, egal ob auf YouTube, Facebook oder Instagram, handelt es sich nämlich um kommerzielle Kommunikation im Sinne von § 6 Abs. 1 TMG. Diese muss der Betrachter klar als solche erkennen können. Gesponserte Beiträge müssen einen entsprechenden Hinweis enthalten. Zugleich muss kenntlich gemacht werden, in wessen Auftrag diese kommerzielle Kommunikation erfolgt (vgl. § 6 Abs. 1 Nr. 2 TMG). In diesem Zusammenhang muss also das Unternehmen, welches die Kampagne in Auftrag gegeben hat, entsprechend genannt werden. Fehlt die Kennzeichnung (vgl. § 6 Abs. 1 Nr. 1, Nr. 2 TMG), stellt dies zugleich einen Wettbewerbsverstoß dar, denn bei § 6 TMG handelt es sich um eine Marktverhaltensregelung im Sinne von § 3a UWG. Sowohl der Influencer als auch das beworbene Unternehmen können demzufolge von Mitbewerbern als auch der Wettbewerbszentrale wettbewerbsrechtlich auf Unterlassung in Anspruch genommen werden (vgl. über § 8 Abs. 2 UWG).

Unser Kommentar

Das Vorgehen der MA HSH zeigt, dass nicht gekennzeichnete Influencer Beiträge nicht mehr geduldet werden. Umso wichtiger ist es, im Vorfeld einer Influencer Kampagne mit der Agentur und/oder direkt mit dem Influencer vertraglich zu regeln, dass die Beiträge zu kennzeichnen sind. Zwar herrscht noch eine gewisse Unsicherheit darüber, wie genau ein Beitrag zu kennzeichnen ist. Die Landesmedienanstalten haben aber mittlerweile einen Leitfaden herausgebracht, unter welchen Voraussetzungen zumindest sie selbst einen Beitrag als ausreichend gekennzeichnet erachten. Zwar sind Gerichte im Rahmen eines wettbewerbsrechtlichen Verfahrens an diesen Leitfaden nicht gebunden. Allerdings spricht vieles dafür, dass von einer ausreichenden Kennzeichnung ausgegangen werden kann, soweit die der Vorgaben der Landesmedienanstalten eingehalten werden. Im Zweifel sollte genau geprüft werden, ob die Kennzeichnung ausreichend ist, um dem Vorwurf der Schleichwerbung zu entgehen.

Drittinhalte auf Webseiten in Gefahr: Gefällt Facebooks „Gefällt mir“ den Gerichten?

OLG Düsseldorf, Vorlagebeschluss vom 19. Januar 2017, Az.: I-20 U 40/16

Auf den Punkt.

Die Einbindung des „Gefällt mir“-Buttons von Facebook bleibt weiterhin mit rechtlichen Risiken verbunden. Bisher konnte ein Abmahnrisiko durch den Einsatz bestimmter Lösungen (2-Klick-Lösung, „Shariff“-Lösung etc.) reduziert werden. Solche Lösungen sollen die Übertragung von Daten aufgrund des Buttons von einer Entscheidung des Internetnutzers abhängig machen. Der EuGH soll nun unter anderem klären, welche Anforderungen dabei an die Informationspflichten und die einzuholende Einwilligung zu stellen sind. Die Entscheidung wird auch für sonstige Inhalte von Drittanbietern relevant, die Daten wie die IP-Adresse übertragen.

Hintergrund

Bereits 2015 mahnte die Verbraucherzentrale NRW die Fashion ID GmbH & Co. KG (Online-Shop der Peek & Cloppenburg KG Düsseldorf) wegen der Verwendung des “Gefällt mir”-Buttons von Facebook auf deren Webseiten ab. Wird eine Webseite aufgerufen, auf welcher der “Gefällt mir”-Button integriert ist, fordert der Browser des Internetnutzers den Inhalt (d.h. den Code) für den Button von Facebook an. Eine Interaktion mit dem Button (z.B. ein Anklicken, Eingabe von Daten in eine Maske, etc.) ist dafür nicht notwendig. Dabei teilt der Browser automatisch bei Aufruf der Webseite dem Server von Facebook die IP-Adresse sowie weitere technische Informationen mit. Welche Informationen der Browser konkret übermittelt und Facebook mit diesen Informationen weiter verfährt, kann der Anbieter der Webseite (hier: Fashion ID GmbH & Co. KG) nicht beeinflussen. Beispielsweise kann

Facebook die Informationen dauerhaft speichern oder für ein Profil des Internetnutzers auswerten. Nachdem die Fashion ID GmbH & Co. KG den Button nicht entfernte, kam es zum Gerichtsverfahren vor dem LG Düsseldorf. Dort obsiegte die Verbraucherzentrale zumindest mit 3 von 4 Klageanträgen. Nun lag der Fall in der Berufung dem OLG Düsseldorf zur Entscheidung vor.

Der Fall

In der Berufung vor dem OLG Düsseldorf bekam die Fashion ID GmbH & Co. KG Unterstützung von Facebook Irland als Streithelferin. Im Rahmen des Verfahrens wurde bekannt, dass der Browser beim Abruf des „Gefällt mir"-Buttons neben der IP-Adresse und ggf. dem sog. Browser-String mehrere Cookies übermittelt:

1. den Session Cookie, der bei eingeloggten Facebook-Mitgliedern gesetzt ist und der eine eindeutige Zuordnung zu einem bestimmten Facebook-Nutzer ermöglicht;

2. den „datr"-Cookie, der beim ersten Besuch einer Facebook-Seite gesetzt wird und bei Mitgliedern und Nichtmitgliedern eine Zuordnung zu einem bestimmten Browser ermöglicht;

3. den „fr"-Cookie, der ebenfalls eine Identifizierung des Nutzers erlaubt, und der beim Besuch einer Facebook-Seite oder einer – nicht näher benannten – Partnerseite gesetzt wird.

Darüber hinaus wird auch die Seite an Facebook übermittelt, von der aus der Button aufgerufen wird.

Im Berufungsverfahren hat Facebook Irland erstmals vorgetragen, die an Facebook übermittelte IP-Adressen deutscher Seitenbesucher sofort nach Eingang zu anonymisieren. Eine Auswertung erfolge ausschließlich über Cookies, die nur bei registrierten Facebook-Nutzern gesetzt werden würden. Die Verbraucherzentrale NRW sieht darin einen Verstoß gegen deutsches und europäisches Datenschutzrecht. Voraussetzung sei die ausdrückliche bzw. informierte Einwilligung der Betroffenen. Nicht ausreichend sei ein bloßer Hinweis in der Datenschutzerklärung, dass eine Weiterleitung von Daten an Facebook erfolge, auf deren Umfang ein Webseitenbetreiber keinen Einfluss habe. Gleichsam sei ein Verweis auf die Datenschutzbestimmungen von Facebook ungenügend. Das geltende Datenschutzrecht verlange eine transparente Aufklärung über die Datensammlung und –verwertung.

Die Entscheidung

Das OLG Düsseldorf hat beschlossen, hierzu Vorlagefragen an den EuGH zu übergeben. Mit den Vorlagefragen möchte das OLG Düsseldorf im Hinblick auf die „inhaltlichen" datenschutzrechtlichen Vorgaben des EU-Rechts vom EuGH im Wesentlichen klären lassen,

- ob ein Webseitenbetreiber der „für die Verarbeitung Verantwortliche" bleibt, wenn er selbst den Datenverarbeitungsvorgang aufgrund von Drittinhalten nicht beeinflussen kann?
- ob ein Webseitenbetreiber, falls er nicht „für die Verarbeitung Verantwortlicher" sein sollte, überhaupt zivilrechtlich in Anspruch genommen werden kann?
- ob es bei einer Abwägung der „berechtigten Interessen" auf das Interesse des Webseitenbetreibers an der Einbindung von Drittinhalten oder auf das Interesse des Dritten ankomme, dessen Inhalte eingebunden werden?
- wer eine Einwilligung des Betroffenen erhalten müsse – der Webseitenbetreiber oder der Dritte, dessen Inhalte eingebunden werde)?
- ob den Webseitenbetreiber besondere Informationspflichten treffen, sofern er die Ursache für die Verarbeitung personenbezogener Daten durch die Einbindung der Drittinhalte setzt?

Zudem möchte das OLG Düsseldorf vom EuGH klären lassen, ob die Verbraucherzentrale NRW die behaupteten Verstöße überhaupt geltend machen darf. Denn die Verbraucherzentrale NRW nimmt dafür als gemeinnütziger Verband zur Wahrung der Interessen der Verbraucher eine deutsche Regelung in Anspruch, die gegen das Unionsrecht verstoßen könnte (Art. 22, 23 und 24 RL 95/46/EG). Erst wenn die Beantwortung dieser Vorlagefragen vorliegt, wird das OLG Düsseldorf das Berufungsverfahren entscheiden.

Unser Kommentar

Eine Beantwortung der Vorlagefragen bzw. die Fortsetzung des Verfahrens vor dem OLG Düsseldorf ist kurzfristig nicht zu erwarten. Für die Praxis bedeutet dies, dass auch weiterhin Rechtsunsicherheit besteht. Es ist nicht auszuschließen, dass etwa die Verbraucherzentralen weiter gegen die Verwendung der „Gefällt mir"-Buttons von Facebook auf Webseiten vorgehen werden. Ein solches Risiko ließe sich mit Hilfe der seit Anfang 2014 etablierte 2-Klick-Lösung oder deren Nachfolger („Shariff"-Lösung) allenfalls reduzieren. Außerdem steht der „Gefällt mir"-Button von Facebook hier als Stellvertreter für alle Drittinhalte, die auf einer Webseite eingebunden sind und

die durch den Browser des Nutzers automatisch von Servern Dritter heruntergeladen werden. Beispielsweise erfolgt auch bei YouTube- oder Google Maps Inhalten regelmäßig eine Kommunikation mit dem YouTube / Google-Server ohne eine bewusste Freigabe, umfassende Belehrung oder Einholung einer Einwilligung des Internetnutzers. Die weitere Entwicklung des Verfahrens hat also weitreichende Bedeutung für alle Webseitenbetreiber, die solche Drittinhalte in ihre Webseite integrieren. Die Verbraucherzentrale NRW hat damit einem Grundelement des modernen Internets (gewollt oder ungewollt) den Kampf angesagt. Einschränkend ist jedoch zu berücksichtigen, dass im Mai 2018 die Datenschutzgrundverordnung sowie daneben die Privacy-Verordnung in Kraft treten werden, mit denen das geltende Datenschutzrecht umfassend neu gestaltet wird.

Zum Zu-Eigen-Machen von Äußerungen durch den Betreiber eines Bewertungsportals

BGH, Urteil vom 4. April 2017, Az.: VI ZR 123/16

Auf den Punkt.
Der Betreiber eines Bewertungsportals, der die Bewertung eines Nutzers ändert und ohne Rücksprache mit dem Nutzer entscheidet, welche Äußerungen der Bewertung er abändert, entfernt oder beibehält, übernimmt die Verantwortung für den Inhalt der geänderten Bewertung.

Hintergrund

Der Beklagte betreibt ein Bewertungsportal für Kliniken, in das Patienten ihre Bewertung einstellen können. Nach seiner Operation hatte ein Patient einen Erfahrungsbericht über die Klinik in das Bewertungsportal eingestellt. In seinem Bericht behauptete der Patient, es sei „bei“ einem Standardeingriff zu einer septischen Komplikation gekommen. Das Klinikpersonal sei mit der lebensbedrohlichen Notfallsituation überfordert gewesen. Beinahe habe dies zu seinem Tod geführt. Die Klägerin ist die Betreiberin der Klinik. Sie forderte den Beklagten auf, den Beitrag aus dem Portal zu entfernen. Daraufhin änderte und ergänzte dieser eigenständig, ohne weitere Rücksprache mit dem Patienten, den Text der Bewertung. Hiergegen klagte die Klägerin beim Landgericht Frankfurt am Main auf Unterlassung. Das Landgericht hat der Klage stattgegeben. Das OLG Frankfurt bestätigte die Entscheidung des Landgerichts.

Die Entscheidung

Auch der BGH bejahte den Unterlassungsanspruch der Klägerin. Der Beklagte habe sich die angegriffenen Äußerungen zu eigen gemacht. Deshalb hafte er als unmittelbarer Störer. Dies begründeten die Richter damit, dass der Beklagte die Äußerungen des Patienten inhaltlich überprüft und beeinflusst habe. Er habe nämlich selbstständig, ohne Rücksprache mit

dem Patienten, entschieden, welche Äußerungen er abändere oder entferne und welche er beibehalte. Diesen Umgang mit der Bewertung habe er der Klägerin auch mitgeteilt. Bei der gebotenen objektiven Sicht aufgrund einer Gesamtbetrachtung aller Umstände habe der Beklagte damit die inhaltliche Verantwortung für die angegriffenen Äußerungen übernommen. Da es sich bei den Äußerungen um unwahre Tatsachenbehauptungen und um Meinungsäußerungen auf unwahrer Tatsachengrundlage und mit unwahrem Tatsachenkern handele, habe das Recht des Beklagten auf Meinungsfreiheit hinter dem allgemeinen Persönlichkeitsrecht der Klägerin zurückzutreten.

Kommentar

Grundsätzlich sind auch negative Bewertungen in Bewertungsportalen unzulässig, wenn es sich um unwahre Tatsachenbehauptungen handelt. Der Betreiber von Bewertungsportalen haftet jedoch nur begrenzt für fremde Inhalte, wenn er zumutbare Prüfpflichten verletzt hat. Dabei forderte der BGH in jüngster Zeit von Betreibern von Ärzte-Bewertungsportalen bereits erhöhte Prüfungspflichten, da solche Portale ein gesteigertes Risiko für Persönlichkeitsverletzungen aufweisen. Im vorliegenden Fall haftet der Portalbetreiber bereits uneingeschränkt als unmittelbarer Störer, da er sich selbst die Äußerung des Patienten zu eigen gemacht hat. Offen bleibt, ob jede Änderung von Erfahrungsberichten zu einem solchen unmittelbaren Anspruch gegen den Portalbetreiber führt.

Bösgläubigkeit einer Markenanmeldung

BPatG, Beschluss vom 5. Juli 2016,
Az.: 24 W (pat) 10/14)

Auf den Punkt.
Das Bundespatentgericht (BPatG) hat entschieden, dass die Löschung einer Marke wegen Nichtigkeit aufgrund der Annahme einer bösgläubigen Markenanmeldung nur nach einer umfassenden Interessenabwägung erfolgen darf. Dabei können Aspekte wie das Verhältnis der Parteien zueinander oder die Tatsache, ob die Marke durch einen anderen (sog. Strohmann) angemeldet wurde, relevant werden.

Hintergrund

Gegenstand der Entscheidung war ein Löschungsantrag gegen die Marke „Yogilotus“. Die Parteien sind Wettbewerber im Bereich des Online-Vertriebs von Yoga-Artikeln. Die Marke hatte die Inhaberin nicht selbst, sondern durch einen Strohmann angemeldet. Die Antragstellerin beantragte die Löschung der Marke wegen Nichtigkeit und stützte ihr Vorbringen auf das Vorliegen einer bösgläubigen Anmeldung. Sie hatte kurz vor der Anmeldung selbst Produkte auf ihrer Website unter der Bezeichnung „Yogilotus“ veröffentlicht. Die Markeninhaberin könnte grundsätzlich gegen eine solche Veröffentlichung aus der nicht gelöschten Marke vorgehen.

Das DPMA gab dem Löschungsantrag statt und verfügte die Marke zu löschen. Gegen diese Entscheidung legte die Markeninhaberin Beschwerde ein, über welche das BPatG nunmehr zu entscheiden hatte. Sie regte in diesem Zusammenhang an, die Rechtsbeschwerde vor dem BGH zu der Frage zuzulassen, ob aus dem Tätigwerden eines Strohmannes auf eine Bösgläubigkeit geschlossen werden könne. Und ferner, inwieweit dabei eine Benutzungsabsicht der hinter dem Strohmann stehenden Person an der Marke zu berücksichtigen sei.

Die Entscheidung

Das BPatG hat die Beschwerde als unbegründet zurückgewiesen und damit die Löschung der Marke bestätigt. Nach Auffassung des BPatG war die Markenanmeldung bösgläubig. Das Gericht stellte klar, dass der Anmelder einer Marke nicht schon dann bösgläubig handelt, wenn er weiß, dass ein anderer dasselbe Kennzeichen für Waren im Inland nutzt, ohne jedoch hierfür einen entsprechenden formalen Kennzeichenschutz erworben zu haben. Vielmehr kann Bösgläubigkeit nur dann gegeben sein, wenn besondere Umstände vorliegen, die die Erwirkung des Zeichenschutzes als sittenwidrig oder rechtsmissbräuchlich erscheinen lassen. Dies ergibt sich aus einer umfassenden Interessenabwägung im Einzelfall. Das BPatG kam dabei zu dem Ergebnis, dass die Markenanmeldung vorliegend in erster Linie erfolgte, um die wettbewerbliche Entfaltung der Löschungsantragstellerin zu beeinträchtigen. Hierfür sprachen im vorliegenden Fall gleich eine Reihe von Indizien: Die Markeninhaberin kannte unstreitig die Vorbenutzung durch die Löschungsantragstellerin. Zudem konkurrierten die Parteien seit geraumer Zeit miteinander, was sich auch in zahlreichen wettbewerbsrechtlichen Auseinandersetzungen zeigte. Darüber hinaus hatte ein Vertreter der Markeninhaberin zuvor sinngemäß verkündet, dass dann „wohl andere Saiten aufgezogen werden müssten“. Ferner versuchte die Markeninhaberin auch, Warenzulieferer der Löschungsantragstellerin abzuwerben, um augenscheinlich den Druck zu erhöhen. Letztlich würdigte das BPatG auch die Einschaltung eines Strohmanns zu Lasten der Markeninhaberin. Diese ist zwar nicht grundsätzlich ein Indiz für Bösgläubigkeit, jedoch kam im vorliegenden Fall hinzu, dass insgesamt sechs verschiedene, zuvor von der Löschungsantragstellerin auf ihrer Website verwendete Begriffe, durch die Markeninhaberin als Marke angemeldet worden waren. Dabei hatte die Markeninhaberin für vier der sechs Anmeldungen durch den Strohmann die Anmeldegebühr gezahlt. Das BPatG kam aufgrund der zahlreichen Indizien zu dem Schluss, dass die Markeninhaberin die Anmeldungen gerade deshalb veranlasst hatte, weil die Zeichen durch die Löschungsantragstellerin bereits zuvor verwendet wurden. Daher musste folgerichtig auch die Interessenabwägung zu dem Ergebnis kommen, dass die Anmeldung bösgläubig mit unlauterer Behinderungsabsicht erfolgte. In einem solchen Fall ist die Löschung der Marke gerechtfertigt, denn sie stellt einen verhältnismäßigen Eingriff in die eigentumsrechtliche Stellung des Markeninhabers dar. Offen blieb, ob aus der Strohmanntätigkeit auf das Vorliegen der behaupteten Bösgläubigkeit geschlossen werden könne. Außerdem, inwieweit eine Benutzungsabsicht der hinter dem tätig werdenden Strohmann stehenden Person zu berücksichtigen sei. Für die Zulassung der Rechtsbeschwerde und Klärung dieser Frage sah das BPatG im konkreten Fall keinen Anlass. Die Strohmanneigenschaft war nur einer von vielen Gesichtspunkten für die Beurteilung der Bösgläubigkeit.

Unser Kommentar

Das BPatG hat sich mit der Frage beschäftigt, unter welchen Voraussetzungen die Bösgläubigkeit einer Markenanmeldung angenommen werden kann. Es hat dabei abermals deutlich gemacht, dass der Frage eine umfassende Interessenabwägung im Einzelfall zu Grunde zu legen ist. Zu Recht hat das BPatG von der Zulassung der Rechtsbeschwerde bezüglich der Auswirkungen der Strohmanntätigkeit mangels Vorliegens einer grundsätzlichen Rechtsfrage abgesehen. Insbesondere war im vorliegenden Fall die Strohmanntätigkeit nur einer von mehreren Gesichtspunkten, die zur Annahme der Bösgläubigkeit führten. Auch zukünftig besteht daher grundsätzlich zunächst kein alleiniges Risiko darin, eine Marke durch einen Strohmann anzumelden.

“Googlen reicht“: Anforderungen an vergleichende Werbung im Internet

OLG Frankfurt, Urteil vom 22. September 2016, Az.: 6 U 103/15

Auf den Punkt.
Im Rahmen einer vergleichenden Werbung gegenüber Verbrauchern im Internet reicht es für die notwendige Nachprüfbarkeit der Werbeaussage aus, dass der Vergleich von Produkten leicht in Erfahrung gebracht werden kann. Dies kann auch aufgrund ergänzender Nachforschungen geschehen, wie etwa einer unkomplizierten Recherche im Internet. Nicht notwendig ist dafür, dass ein Verbraucher die Nachprüfbarkeit schon aufgrund der Angaben in der Werbung selbst nachvollziehen kann.

Hintergrund

Die Klägerin nahm die Beklagte auf Unterlassung wegen eines aus ihrer Sicht unzulässigen Werbevergleichs in Anspruch. Die Beklagte hatte ihr eigenes Kosmetikprodukt als preisgünstige, gleichwertige Alternative zum Kosmetikprodukt der Klägerin beworben. In der Werbung wurden jedoch die Preise der beiden Produkte nicht ausdrücklich gegenübergestellt. Das Produkt der Beklagten war im Internet für EUR 180,10 EUR erhältlich, während das Produkt der Klägerin EUR 220,50 kostete. Die Klägerin nahm die Beklagte auf Unterlassung der vergleichenden Werbung, Auskunftserteilung sowie Zahlung von Schadensersatz in Anspruch.

Die Entscheidung

Das OLG Frankfurt sah diese vergleichende Werbung als zulässig an: Nicht beanstandet wurde insbesondere der Preisvergleich, ohne einen Preis in der Werbung selbst zu nennen. Das Gericht ging von der funktionellen Gleichwertigkeit der Produkte aus und nannte als Maßstab für eine solche Gleichwertigkeit das Vorliegen einer wesentlichen Eigenschaft bzw. die Tauglichkeit der Produkte zu einem bestimmten Zweck. Letztlich musste hierzu aber keine Entscheidung getroffen werden, da die Klägerin den Darlegungen der Beklagten in diesem Punkt nicht substantiiert entgegengetreten war.

Hinsichtlich der Aussage „preiswerte Alternative“ führte das Gericht aus, dass die Adressaten der Werbung bzw. die angesprochenen Verkehrskreise darunter verstehen, dass das Produkt der Beklagten günstiger sei als das der Klägerin. Die Preise müssen hierfür nicht unmittelbar in der Werbung genannt und gegenübergestellt werden. Vielmehr reiche es aus, dass aus der Werbeaussage hervorgehe, welche Produkte im Einzelnen gegenübergestellt werden, so dass der Adressat der Werbung die Bestandteile des Vergleichs leicht in Erfahrung bringen könne. Damit soll er selbst, ggf. auf der Grundlage ergänzender Nachforschungen durch einen Dritten, überprüfen können, ob diese tatsächlich wahr sind. Werden beide Produkte im Internet vertrieben, sei es Verbrauchern grundsätzlich ohne weiteres möglich, die Preise durch eine eigene Internetrecherche („Google“ etc.) herauszufinden und auch die funktionelle Gleichwertigkeit selbst zu prüfen bzw. prüfen zu lassen. Etwas anderes kann für Werbung gelten, die sich an Fachkreise richtet. Hier können weitere Angaben erforderlich sein, um die notwendige Klarheit zu bringen und den Werbevergleich zu erläutern.

Im Ergebnis wurde der Klägerin aus einem anderen Grund Recht gegeben. Das Gericht untersagte die Werbung aufgrund irreführender Angaben. Die Darstellung der Werbung zeigte unmittelbar oberhalb des Werbetextes Produkte, die gar nicht Bestandteil des Angebots der Beklagten waren.

Unser Kommentar

Diese Entscheidung des OLG Frankfurt ist zu begrüßen, da die Anforderungen an den Werbenden nicht „überspannt“ werden. Zwar wird den Werbenden (nach zwischenzeitlich erfolgter Liberalisierung des Wettbewerbsrechts) das Leben wieder zunehmend aufgrund (europäischer) Vorgaben aus Brüssel schwer gemacht. Die vorliegende Entscheidung bevormundet aber weder die Verbraucher, die durchaus in der Lage sind, die Preise der Produkte zu überprüfen, noch schützt sie Unternehmen vor einem lediglich unliebsamen Werbevergleich, der jedoch keine rechtlichen Grenzen überschreitet. Sind Werbeaussagen im Hinblick auf die Gleichwertigkeit oder den Vergleich der Preise unzutreffend, kann die Werbung aufgrund einer Irreführung untersagt werden. Damit werden sowohl Verbraucher als auch Wettbewerber ausreichend geschützt.

eIDAS-Verordnung: Neue Spielregeln für die elektronische Identifikation

Auf den Punkt.

Seit dem 1. Juli 2016 gilt die eIDAS-Verordnung im Europäischen Wirtschaftsraum und ersetzt somit weite Teile des bis dahin maßgeblichen Signaturgesetzes. Hieraus ergeben sich geänderte Anforderungen für die Anbieter von Online-Identifizierungsdiensten. Zugleich wird der unionsweite Einsatz von elektronischen Signaturen und anderen digitalen Vertrauensdiensten erheblich vereinfacht. Dies dürfte insbesondere dem Markt für Online-Kreditverträge neue Impulse geben.

Hintergrund

Bisher richtete sich der Einsatz von digitalen Identifizierungsmitteln, wie der qualifizierten elektronischen Signatur, nach nationalem Recht. Im Wesentlichen wurde darin die europäischen Richtlinie 1999/93/EG (Signaturrichtlinie) umgesetzt. In Deutschland war insofern das Signaturgesetz (SigG) als korrespondierender Umsetzungsakt maßgeblich. Um die teilweise divergierenden nationalen Umsetzungsakte zu vereinheitlichen, trat zum 17. September 2014 die Verordnung (EU) Nr. 910/2014 (eIDAS-Verordnung) in Kraft, die einheitliche Rahmenbedingungen für die digitale Identifizierung enthält. Seit dem 1. Juli 2016 entfaltet die Verordnung unmittelbare rechtliche Wirkungen in allen Mitgliedstaaten.

Wesentliche inhaltliche Neuerungen durch eIDAS

Die nationalen Umsetzungsakte enthielten bisher unterschiedliche Anforderungen an digitale Vertrauensdienste, die sich mit der Identifizierung von Personen bzw. deren Teilnahme am Abschluss von Verträgen im Internet befassen. Diese Diskrepanz wurde besonders deutlich bei Einbindung mobiler Endgeräte in den Erstellungsprozess elektronischer Signaturen: Nach deutschem Signaturrecht wurde dies bisher überwiegend für unzulässig erachtet, da sich die Signaturerstellungseinheit im Machtbereich des Signierenden befinden müsse (§ 5 Abs. 6 SigG).

Derartige Regelungsunterschiede resultierten aus den Gestaltungsspielräumen bei der Umsetzung der Signaturrichtlinie in nationales Recht; diese sind aber im „digitalen Binnenmarkt“ der EU nicht erwünscht. Folgerichtig finden sich nun in der eIDAS-Verordnung einheitliche Regelungen zu digitalen Vertrauensdiensten. Diese Begrifflichkeit referenziert das englische Original „trust services“ und betrifft insbesondere die bereits angesprochene Erstellung (qualifizierter) elektronischer Signaturen; aber auch (derzeit noch) weitaus weniger populäre Instrumente wie das elektronische Einschreiben oder den elektronischen Zeitstempel.

Als zentrale inhaltliche Änderung erfolgt die ausdrückliche einheitliche Anerkennung der sog. Fernsignaturen, bei denen sich die Signaturerstellungseinheit gerade nicht im Machtbereich des Signierenden befinden muss (Erwägungsgrund 52 eIDAS-VO). In der Praxis dürfte dies die Verbreitung dieses Instruments wesentlich befördern, da nun dem Grunde nach auch etwa eine Signaturerstellung per Mobiltelefon in Betracht kommt. Über dieses werden die meisten potentiellen Nutzer bereits verfügen, anders als über eine sperrige, konventionelle Erstellungseinheit wie beispielsweise einen Card Reader.

Gerade beim Abschluss von Online-Verträgen stellt die Feststellung der Identität des Vertragspartners bzw. die Prüfung der Echtheit von „Unterschriften“ eine große praktische Hürde dar. Daher finden sich in der Verordnung auch Regelungen zum Beweiswert der elektronischen Instrumente, um auch auf diesem Sektor eine Vereinheitlichung zu erreichen: Grundsätzlich sollen rechtskonform erstellte, digitale Kennzeichen einen Anscheinsbeweis im nationalen Prozessrecht begründen, dass ein solches Kennzeichen inhaltlich unversehrt und auch tatsächlich vom Berechtigten erstellt worden ist (vgl. Art. 35 Abs. 2 eIDAS). Auch dies dürfte die Verbreitung derartiger Instrumente fördern. Interessanterweise enthält die Verordnung zum praktisch wichtigsten Instrument, der qualifizierten elektronischen Signatur, keine Beweisregel. Dies liegt im Wesentlichen daran, dass eine entsprechende Regelung bereits in der Signaturrichtlinie enthalten war, die in Deutschland in Form des § 371a ZPO bereits in nationales Recht umgesetzt worden ist.

Ein weiterer wesentlicher Regelungsaspekt betrifft die einheitliche Geltung von Kennzeichen im gesamten EWR, beispielsweise der qualifizierten elektronischen Signatur. Zwar kannten auch die Signaturrichtlinie und korrespondierend das deutsche Signaturgesetz (§ 23 SigG) eine Regelung, wonach Signaturen aus dem EU-Ausland u.U. gleichzusetzen waren. Dies jedoch nur, sofern die Einhaltung der jeweiligen nationalen Anforderungen sichergestellt war. Dieses System wird ersetzt durch einheitliche europäische „Vertrauenslisten“, die europaweit eine eindeutige Ermittlung geeigneter Anbieter von

qualifizierten Vertrauensdiensten ermöglichen. Schließlich enthält die Verordnung flankierende Regelungen, zum Beispiel zum erforderlichen IT-Sicherheitsniveau bei Anbieter von Vertrauensdiensten und dem dazugehörigen Notifizierungsverfahren.

Unser Kommentar

Die Vereinheitlichung der Rahmenbedingungen für die Anbieter qualifizierter elektronischer Signaturen und anderer Vertrauensdienste ist zu begrüßen, da hiermit die zentralen Hemmnisse für die Verbreitung dieser modernen digitalen Instrumente abgebaut werden: Einerseits wird der europäische Wettbewerb weiter vereinfacht, indem nun der Sitz des Anbieters letztlich unerheblich ist. Insbesondere aber wird die praktische Nutzbarkeit der Signatur aufgrund der Entkoppelung von der lokalen Signaturerstellungseinheit erheblich aufgewertet. Gerade die „mobile Signatur“ dürfte sich in der Praxis großer Beliebtheit erfreuen. Dies dürfte sich insbesondere in den Bereichen auswirken, die typischerweise mit formbedürftigen Willenserklärungen konfrontiert sind und zugleich darauf angewiesen sind, relativ einfach bzw. günstig eine Masse an Verträgen zu schließen. Zum Beispiel ist im Finanzsektor der online erfolgende Abschluss von Kreditverträgen grundsätzlich formwirksam, sofern eine qualifizierte elektronische Signatur verwendet wird (§ 126a BGB). Durch den Einsatz von Fernsignaturen dürften sich für diesen Sektor massive Wachstumspotentiale eröffnen. Allerdings muss insbesondere bei ausländischen Signaturen darauf geachtet werden, dass sie alle vereinheitlichten Anforderungen erfüllen.

Zugleich hält sich die Verordnung an mehreren Punkten zurück, insbesondere was den Beweiswert von digitalen Signaturen betrifft. Hier findet sich aber ohnehin bereits eine Regelung im deutschen Prozessrecht. Auch schweigt eIDAS zu materiell-rechtlichen Fragen im Zusammenhang mit qualifizierten elektronischen Signaturen: Kann eine Signatur ein Dokument mit mehreren Erklärungen „abdecken“? Welche Dokumente müssen von wem wie gezeichnet und was muss dem Endnutzer letztlich zur Verfügung gestellt werden? Hierbei handelt es sich um Fragestellungen, die im nationalen Recht anhand der einschlägigen Formvorschriften unter Würdigung der Besonderheiten elektronischer Signaturen beantwortet werden müssen. Auf diesem Wege lassen sich im Zusammenspiel mit der eIDAS-Verordnung bereits jetzt durchaus Lösungen mit hoher Rechtssicherheit entwickeln, welche die Einführung neuartiger Signaturmechanismen im Bereich des wirtschaftlich immer wichtiger werdenden Online-Vertragsabschlusses begleiten können.

Update für eHealth: Neue Vorschriften für Medizinprodukte

Auf den Punkt.

Für Medizinprodukte und deren Betrieb bringt das Jahr 2017 eine Reihe regulatorischer Neuerungen. Zu den neuen Pflichten für Betreiber und Anwender von Medizinprodukten gehört nach der Zweiten Verordnung zur Änderung medizinprodukterechtlicher Vorschriften beispielsweise, dass größere Einrichtungen einen Beauftragten für Medizinprodukte als zentralen Ansprechpartner einsetzen und dessen E-Mail-Adresse auf der Internetseite veröffentlichen müssen. Außerdem können Hersteller von Medizinprodukten nun nicht mehr darüber bestimmen, wie oft sicherheits- und messtechnische Kontrollen durchzuführen sind. Große Bedeutung wird die europäische Medical Device Regulation haben, die voraussichtlich im Sommer in Kraft treten und mit einer Übergangsfrist von drei Jahren das geltende Recht maßgeblich verschärfen wird.

Wesentliche Inhalte der Verordnung

Zum 1. Januar 2017 ist die Zweite Verordnung zur Änderung medizinprodukterechtlicher Vorschriften in Kraft getreten, welche die Medizinprodukte-Betreiberverordnung (MPBetreibV) und die Medizinprodukte-Sicherheitsplanverordnung in wesentlichen Teilen neu fasst. Neu ist in der MPBetreibV zunächst, dass die Tätigkeiten im Zusammenhang mit dem Betreiben und Anwenden von Medizinprodukten definiert werden (§ 2 MPBetreibV). Medizinprodukte sind nach dem Medizinproduktegesetz (MPG) u.a. elektronische (eHealth) bzw. mobile Geräte (mHealth) und Software, die für die medizinische Versorgung von Menschen eingesetzt werden. Hierzu kann etwa eine bestimmte Gesundheits- bzw. Fitness-App oder auch eine Software zählen, die in ein Medizinprodukt integriert wird (etwa in Kontaktlinsen für Diabetiker, die den Insulinspiegel messen). Zu den neuen Tätigkeiten gehört insbesondere das Errichten, das Bereithalten, die Instandhaltung und die Aufbereitung von

Medizinprodukten sowie die Durchführung sicherheits- und messtechnische Kontrollen. Die Definition des Betreibers orientiert sich an den bisherigen praktischen Regelungen und trägt auch den unterschiedlichen möglichen Betreiberformen Rechnung. Ausgangspunkt ist dabei die ebenfalls definierte Gesundheitseinrichtung als Einrichtung, einschließlich Rehabilitations- und Pflegeeinrichtungen, in der Medizinprodukte durch medizinisches Personal berufsmäßig betrieben oder angewendet werden. Belegärzte oder andere selbständig für Einrichtungen tätige Leistungserbringer sind wie bisher Betreiber ihrer Medizingeräte, die sie in eine Einrichtung mitbringen. Als Betreiber gilt auch, wer außerhalb von Gesundheitseinrichtungen Medizinprodukte zur Anwendung bereithält, beispielsweise Automatik-Defibrillatoren auf Flughäfen. Die Betreiberpflichten erstrecken sich zudem auf Krankenversicherungen, obwohl sie weiterhin eigentlich keine Betreiber von Hilfsmitteln sind. Dass aber auch sie in hohem Maße an Gesundheitsdaten interessiert sind, hat bereits 2007 zu einer gesetzlichen Beschränkung der Erhebung personenbezogener Gesundheitsdaten bei Dritten (sozialen Netzwerken etc.) geführt (vgl. § 213 VVG). Nach der MPBetreibV müssen sie bei der Versorgung mit Medizinprodukten im häuslichen und privaten Umfeld die Pflichten eines Betreibers wahrnehmen (§ 3 Abs. 2 MPBetreibV) und beispielsweise für die Einhaltung sicherheitstechnischer Kontrollen und regelmäßiger Wartungsarbeiten sorgen. Sie können diese Aufgaben aber an Dritte übertragen, etwa an Sanitätshäuser. Wenn ein Patient ein ihm überlassenes Medizinprodukt für den Aufenthalt in einer Gesundheitseinrichtung mitnimmt, verbleiben die Betreiberpflichten bei der überlassenden Krankenversicherung. Die aufnehmende Gesundheitseinrichtung wird in einem solchen Fall nicht Betreiber des Medizinproduktes.

Gesundheitseinrichtungen mit mehr als 20 Beschäftigten müssen eine entsprechend sachkundige und zuverlässige Person als Beauftragten für Medizinproduktesicherheit als zentrale Kontakt- und Koordinationsperson bestellen. Sie soll nach innen und außen wesentliche Aufgaben für den Betreiber wahrnehmen, u.a. auch gegenüber Behörden, Herstellern und Vertreibern im Zusammenhang mit Risikomeldungen und korrektiven Maßnahmen. Diese Person darf bei der Erfüllung der ihr übertragenen Aufgaben nicht behindert oder benachteiligt werden. Die Gesundheitseinrichtung ist verpflichtet, eine E-Mail-Adresse des Beauftragten für Medizinprodukte auf ihrer Internetseite bekannt zu machen. Soweit Einrichtungen schon entsprechende Strukturen eingerichtet haben, müssen sie diese nun ggf. anpassen.

Die bisherige Betreiberverordnung eröffnete Herstellern verschiedene Möglichkeiten, Umfang und Fristen von Kontrollen in ihrem Sinne zu gestalten. So konnten sie beispielsweise auch für solche Medizinprodukte sicherheitstechnische Kontrollen (STK) vorschreiben, die nicht in der Anlage zur MPBetreibV aufgeführt sind. Diese Vorgaben durch den Hersteller sind nun nicht mehr vorgesehen. Der Betreiber hat für die sicherheitstechnischen Kontrollen die Fristen so festzulegen, dass entsprechende Mängel rechtzeitig festgestellt werden können. Nach der neuen Regelung müssen STK bei den in der Anlage aufgeführten Medizingeräten spätestens alle zwei Jahre durchgeführt werden. Vergleichbares gilt für die messtechnischen Kontrollen (MTK), die nicht in den Zuständigkeitsbereich des Herstellers fallen sollen. Sie sind unabhängig von dessen Vorgaben durchzuführen, wenn sie Medizinprodukte der Anlage 2 der Betreiberverordnung betreffen. Die ordnungsgemäße Durchführung einer MTK wird vermutet, wenn der Leitfaden der Physikalisch-Technischen Bundesanstalt (PTB) beachtet worden ist, der künftig eine zentrale Bedeutung erhält.

Die Zweite Verordnung zur Änderung medizinprodukterechtlicher Vorschriften hat zudem die Medizinprodukte-Sicherheitsplanverordnung an einige aktuelle Gegebenheiten und Erfordernisse angepasst. Dabei ist vor allem die Definition des Vorkommnisses als Auslöser für eine Meldepflicht relevant, die nunmehr auch Mängel der Gebrauchstauglichkeit umfasst.

Die Neuregelungen treten mit einer Ausnahme am 1. Januar 2017 in Kraft. Ausgenommen davon ist eine zum 1. Januar 2020 in Kraft tretende Änderung der MPBetreibV, die sich auf bestimmte Zertifikate bezieht. Werden solche Zertifikate vorgelegt, kann nachgewiesen werden, dass für bestimmte Tätigkeiten die besonderen Anforderungen der MPBetreibV erfüllt werden.

Neuer europäischer Rechtsrahmen für Medizinprodukte

Im Sommer dieses Jahres wird zudem voraussichtlich die Medical Device Regulation (MDR) in Kraft treten. Sie soll mit einer Übergangsfrist von 3 Jahren das bisherige Medizinprodukterecht, insbesondere das nationale Medizinproduktegesetz (MPG) ergänzen und die Richtlinien 93/42 sowie 90/385 für Implantate ablösen. Einer der Gründe hierfür ergab sich aus dem sog. PIP-Skandal. Ein Hersteller hatte in für Brustimplantate Industrie-Silikon anstelle von hochreinen medizinischen Silikons verwendete. Als Folge dieses und anderer Skandale rückte der Bedarf einer stärkeren Kontrolle in den Fokus der Öffentlichkeit und Politik. Die sich derzeit abzeichnenden Konsequenzen des geänderten Rechtsrahmens für Medizinprodukte bestehen unter anderem in einem deutlich erhöhten Dokumentationsaufwand für Hersteller. Marktüberwachungsbehörden können zukünftig die Nichtkonformität von

Medizinprodukten feststellen (vgl. Art. 73 Absatz 1 (d) und (f) MDR). Sorgt der Hersteller daraufhin nicht in angemessener Frist für die Wiederherstellung der Konformität, können Behörden untersagen, dass das Produkt auf dem europäischen Markt bereitgestellt bzw. in Verkehr gebracht wird.

Die wichtigsten Änderungen der Medical Device Regulation:

1. Klassifizierung von Medizinprodukten, insbesondere von Software und mobilen Gesundheits-Apps

Für Medizinprodukte, zu deren Bestandteilen Software gehört, gibt es erhebliche Veränderungen. Grundsätzlich werden Medizinprodukte weiterhin in vier Risikoklassen eingeteilt. Die Klassifizierungsregeln werden allerdings für einzelne Produkte bzw. Produkttypen verändert. Dies gilt etwa für Software, die Informationen für diagnostische oder therapeutische Zwecke liefert. Sofern beispielsweise die unter dem Schlagwort des mHealth zusammengefassten Gesundheits-Apps nicht als bloße Wellness Produkte für allgemeine Zwecke, sondern für medizinische Zwecke bestimmt sind, ist deren Risikopotential besonders zu berücksichtigen. Möglicherweise ist bei der Konformitätsbewertung eine Benannte Stelle hinzuzuziehen.

2. Sicherheitsanforderungen für Software im Medizinprodukt

Insbesondere für Ärzte und Krankenhäuser dürften die folgenden Regelungen der Allgemeinen Sicherheits- und Leistungsanforderungen für Software im Medizinprodukt folgenschwer sein: „Bei Produkten, zu deren Bestandteilen Software gehört, oder bei Produkten in Form einer Software, wird die Software entsprechend dem Stand der Technik entwickelt und hergestellt, wobei die Grundsätze des Software-Lebenszyklus, des Risikomanagements einschließlich der Informationssicherheit, der Verifizierung und der Validierung zu berücksichtigen sind“ (Ziffer 14.2 Anhang I MDR). Zur weiteren Absicherung legt der Hersteller die Anforderungen an Hardware, Eigenschaften von IT-Netzen und IT-Sicherheitsmaßnahmen einschließlich des Schutzes vor unbefugtem Zugriff auf die Software fest, die mindestens gelten müssen (Ziffer 14.3a Anhang I MDR).

3. Strengere Regelungen für Benannte Stellen

Staatlich anerkannte Unternehmen, die als Benannte Stellen Medizinprodukte-Hersteller kontrollieren, müssen mit Geltungsbeginn der MDR neu benannt werden. Das Antragsverfahren und die nachzuweisenden organisatorischen und allgemeinen Anforderungen und die Anforderungen an das Qualitätsmanagement richten sich nach Art. 38 der MDR. Anträge auf Neubenennung können frühestens sechs Monate nach Inkrafttreten der Verordnungen gestellt werden.

4. Verschärfte Anforderungen an den Hersteller

Mit Einführung der MDR müssen klinische Daten auch nach der Markteinführung weiterhin gesammelt, dokumentiert und ausgewertet werden. Bisher war die Datenerhebung mit der Markteinführung beendet. Zur Verbesserung von Gesundheit und Sicherheit sollen Schlüsselelemente des derzeitigen Regulierungskonzepts, beispielsweise die Beaufsichtigung der Benannten Stellen, die Konformitätsbewertungsverfahren, klinische Prüfungen und klinische

Bewertungen, Vigilanz und Marktüberwachung erheblich gestärkt und Bestimmungen zur Gewährleistung von Transparenz und Rückverfolgbarkeit in Bezug auf Medizinprodukte eingeführt werden. Nach Art. 15 der MDR müssen Hersteller zudem eine verantwortliche Person mit entsprechendem Fachwissen vorhalten, die für die Einhaltung der regulatorischen Anforderungen verantwortlich ist.

5. Neues „Scrutiny-Verfahren“

Die MDR führt darüber hinaus ein Prüfverfahren ein (sog. „Scrutiny-Verfahren“). Für bestimmte Hochrisiko-Medizinprodukte soll eine Expertengruppe künftig in den Zertifizierungsprozess eingreifen können, wenn der Verdacht auf Defizite besteht. Betroffen sind beispielsweise Brustimplantate und Herzschrittmacher.

6. Europaweite Datenbank Eudamed und Unique Device Identification (UDI)

Ein Schlüsselelement der MDR ist die Einführung einer zentralen Datenbank „Eudamed“. Mit ihr sollen Informationen über sämtliche Medizinprodukte gesammelt werden, die in der EU im Umlauf sind. Ziel ist es, Transparenz, Zusammenarbeit und Überwachung zu verbessern. Insbesondere Hersteller, Betreiber von Medizinprodukten, Benannte Stellen, Mitgliedstaaten und die EU-Kommission sollen Informationen leichter austauschen können. Dazu sollen in der Datenbank verschiedene Informationen bzw. ganze Datenbanken integriert werden. Für jedes Medizinprodukt wird eine einmalige Nummer vergeben (Unique Device Identification - UDI). Die Nummer hilft dabei, fehlerhafte Produkte leichter zu identifizieren und zurückzuverfolgen.

Bewertung und Ausblick

Das Sicherheitsniveau für den Einsatz von Medizinprodukten unterliegt nach wie vor einem steigenden Anpassungsbedarf an die Risiken, welche die Vermarktung wie auch der Einsatz von Medizinprodukten mit sich bringen kann. So wurden bereits durch die 4. MPG-Novelle die Anforderungen an die klinische Bewertung von Medizinprodukten an das auch bei Arzneimitteln übliche Sicherheitsniveau angepasst. Durch die nunmehr in Kraft getretene Neufassung der Betreiberverordnung soll insbesondere für den Betrieb und die Anwendung von Medizinprodukten ein angemessenes Sicherheitsniveau gewährleisten sollen. Unter anderem für die Hersteller von Medizinprodukten wird die europarechtliche Neufassung der MDR einen erheblichen Umstellungsbedarf mit sich bringen. Sie sollten schon frühzeitig tätig werden und sich für diese neuen Anforderungen wappnen. Dafür beginnt mit dem Inkrafttreten der MDR eine Übergangsfrist von drei Jahren, innerhalb derer sich Hersteller wahlweise noch nach altem oder neuem Recht zertifizieren lassen können. Bis Mitte 2020 bereits ausgestellte Alt-Zertifikate sollten maximal weitere fünf Jahre gültig bleiben. Unklar ist derzeit noch nach Einschätzung des Bundesverbandes der Medizinprodukteindustrie, inwieweit mit dem Ablauf der Übergangszeit etwa für Anzeigepflichten und die Marktüberwachung in jedem Fall neues Recht anzuwenden sein wird.

Veranstaltungen

Termin	Thema/Referent	Veranstalter/Ort
18.05.2017	**IT NRW SAM-Training** Information und Technik Nordrhein-Westfalen (IT.NRW) *(Christian Kuß, LL.M.)*	Düsseldorf
22.05.2017	**IT-Sicherheit** NRW-Bank *(Christian Kuß, LL.M.)*	Düsseldorf
29.05.2017	**Digital Compliance** Management Circle Seminar *(Christian Kuß, LL.M.; Christoph Maiworm)*	Management Circle AG München
19.06.2017	**Crashkurs IT-Recht** Management Circle Intensiv-Seminar *(Christian Kuß, LL.M.; Christoph Maiworm)*	Management Circle AG
28.06.2017	**Digital Compliance** Management Circle Seminar *(Christian Kuß, LL.M.; Christoph Maiworm)*	Management Circle AG Köln
17.07.2017	**Digital Compliance** Management Circle Seminar *(Christian Kuß, LL.M.; Christoph Maiworm)*	Management Circle AG Frankfurt

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.