LANCOM Systems

Allgemeines Informationspaket zum Thema:

„Haftung gewerblicher WLAN-Hotspot-Betreiber für Urheberrechtsverletzungen durch Hotspot-Nutzer“

Inhalt:

Dieses allgemeine Informationspaket wurde im Auftrag der LANCOM Systems GmbH durch Herrn Rechtsanwalt Dr. Jaeschke als Fachanwalt für Gewerblichen Rechtsschutz erstellt (vgl. heise.de, hotelier.de). Die Nutzung ist ausschließlich Partnern und Kunden der LANCOM Systems GmbH sowie im Zusammenhang mit LANCOM Projekten gestattet.

Geltungsbereich ist die Bundesrepublik Deutschland.

Das Informationspaket inklusive der Muster-AGB ist mit größter Sorgfalt erstellt, erhebt jedoch keinen Anspruch auf Vollständigkeit und Richtigkeit. Es stellt keine Rechtsberatung dar und ersetzt im Einzelfall nicht die Beratung durch einen Anwalt. Ein Haftungsanspruch aufgrund der Verwendung der Informationen und Muster-AGB durch Kunden der LANCOM Systems GmbH gegenüber der LANCOM Systems GmbH ist ausgeschlossen.

Die Muster-AGB wurden explizit für die Verwendung mit der LANCOM Public-Spot Option entwickelt. Die rot hervorgehobenen Passagen müssen individuell angepasst werden. Zudem sind manche WLAN/Hotspot-Anbieter verpflichtet, eine Meldung nach § 6 TKG an die Bundesnetzagentur in Bezug auf den gewerblichen Betrieb von öffentlichen Telekommunikationsdiensten zu machen.

Würselen, den 23.02.2011

„Haftung gewerblicher WLAN-Hotspot-Betreiber für Urheberrechtsverletzungen durch Hotspot-Nutzer“

- Kurzfassung -

RA Dr. Lars Jaeschke, LL.M. (Fachanwalt für Gewerblichen Rechtsschutz)

JAESCHKE
MARKEN- UND MEDIENRECHT

Gegenstand kritischer Würdigung dieses Kurzgutachtens ist die Frage der Haftung gewerblicher WLAN-Hotspot-Betreiber für Urheberrechtsverletzungen durch Hotspot-Nutzer. Die nachstehenden allgemeinen Ausführungen ersetzen nicht die Rechtsberatung im konkreten Einzelfall.

- **Zusammenfassung**

  Die Frage der Haftung gewerblicher WLAN-Hotspot-Betreiber für Urheberrechtsverletzungen durch Hotspot-Nutzer ist noch ungeklärt.

  Der Bundesgerichtshof (BGH) hat jedoch in seinem „Filesharing"-Urteil vom 12.05.2010 zur Haftung von Privatpersonen für Urheberrechtsverletzungen durch unerlaubtes Filesharing Hinweise gegeben, die darauf schließen lassen könnten, dass der BGH gewerbliche WLAN-Betreiber privilegieren würde, hätte er über eine solche Konstellation zu entscheiden. Sinnvoll ist es derzeit, Kunden und Mitarbeitern ein, ggf. zeitlich begrenztes und ausreichend sicheres, Passwort („Ticket") zuzuteilen, um unbefugten Dritten möglichst keinen Zugriff zu ermöglichen. Eine Kennungsvergabe an die Benutzer zu dem Zweck, die Benutzer auch zu überwachen ist jedoch aufgrund des weitreichenden Fernmeldegeheimnisses unzulässig. Selbst wenn der BGH keine umfassende Haftungsprivilegierung annehmen sollte, scheiterte eine Haftung kommerzieller WLAN-Betreiber regelmäßig an der Unzumutbarkeit bzw. der rechtlichen Unmöglichkeit der Verhinderung weiterer Verstöße.

  Zu begrüßen ist insoweit ein Urteil des LG Frankfurt am Main vom 18.08.2010,[1] wonach Hotels und damit letztlich auch andere Access-Provider nicht für das unerlaubte Filesharing von Gästen haften.

  Aufgrund der derzeit noch bestehenden Rechtsunsicherheit, stellt sich die Frage, wie abgemahnte Unternehmen konkret auf eine urheberrechtliche Abmahnung wegen unerlaubten Filesharings reagieren sollten. Obgleich es auf den Einzelfall ankommt, liegen 2 Reaktionsmöglichkeiten nahe. Im Einzelnen wird hierzu auf die Übersicht

  „Konkrete Handlungsmöglichkeiten für gewerbliche WLAN-Hotspot-Betreiber nach Erhalt einer Abmahnung wegen Urheberrechtsverletzung"

  verwiesen.

[1] LG Frankfurt am Main, Urteil vom 18.08.2010, Az: 2-6 S 19/09; abrufbar unter www.ipjaeschke.de ; Vorinstanz: AG Frankfurt am Main, Urteil vom 25.09.2009, Az. 31 C 266/08-16

I. Privilegierung gewerblicher WLAN-Anbieter nach § 8 Telemediengesetz (TMG)[2]

Fraglich ist zunächst, ob gewerbliche WLAN-Anbieter durch das Telemediengesetz umfassend privilegiert sind.

Nach § 8 Abs. 1 TMG (Durchleitung von Informationen) sind Diensteanbieter für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich, sofern sie die Übermittlung nicht veranlasst, den Adressaten der übermittelten Informationen nicht ausgewählt und die übermittelten Informationen nicht ausgewählt oder verändert haben. Nach § 7 Abs. 2 TMG besteht keine Verpflichtung, die vermittelten Informationen zu überwachen.

1. Gewerbliche WLAN-Hotspot-Betreiber als Access-Provider

„Diensteanbieter“ im Sinne des TMG ist jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt (§ 2 Satz 1 Nr. 1 TMG).

Dies trifft auf Anbieter eines gewerblichen WLAN-Hotspot (z.B. Hotel oder Gaststätten-WLAN-Netzes o.ä.) zu. Der Anbieter eines solchen WLAN-Netzes vermittelt lediglich den Zugang zum Internet, wenn über das drahtlose Netz eine Verbindung zum Internet besteht. Gleiches gilt auch für den Betreiber eines Internetcafés. Dass dort in der Regel auch Hardware zur Verfügung gestellt wird, ändert daran nichts.[3] Dabei werden weder Adressaten noch Informationen ausgewählt, dies erfolgt ausschließlich durch die Endnutzer.

„Nutzer“ im Sinne des TMG ist jede natürliche oder juristische Person, die Telemedien nutzt, insbesondere um Informationen zu erlangen oder zugänglich zu machen (§ 2 Satz 1 Nr. 3 TMG).

Dies trifft z.B. auf jeden Hotelgast, der das hoteleigene WLAN etc. nutzt, zu.

Der BGH hat sich in seinem „Filesharing“-Urteil vom 12.05.2010[4] jedoch nicht mit der umstrittenen Frage einer Anwendbarkeit von § 8 TMG für WLAN-Netze gewerblicher Anbieter auseinandergesetzt.

---

[2] Telemediengesetz (TMG) vom 26. Februar 2007**,** (BGBl. I S. 179).
[3] *Hoeren/Sieber*, Handbuch Multimedia-Recht, § 8 TMG, Rn. 64.
[4] BGH, Urteil vom 12.05.2010, Az.: I ZR 121/08 – *Sommer unseres Lebens.*

2. Geltung des § 8 TMG für Unterlassungsansprüche

Nach der bisherigen und noch aktuellen Rechtsprechung des BGH[5] gelten die vorgenannten Privilegierungen durch §§ 7, 8 TMG grundsätzlich nicht für den Unterlassungsanspruch bei der Verletzung von Immaterialgüterschutz-rechten.

Im Rahmen des Unterlassungsanspruchs haftet in analoger Anwendung des § 1004 BGB (Beseitigungs- und Unterlassungsanspruch) jeder als Störer für eine Schutzrechtsverletzung, der – ohne selbst Täter oder Teilnehmer zu sein – in irgendeiner Weise willentlich und adäquat kausal an der rechtswidrigen Beeinträchtigung mitgewirkt hat.

Um diese weite Haftung nicht über Gebühr auf Dritte zu erstrecken, die nicht selbst die rechtswidrige Beeinträchtigung vorgenommen haben, wird die Haftung des Störers durch Zumutbarkeitserwägungen im Hinblick auf Prüf- und Handlungspflichten zur Verhinderung und/oder der Störungsbeseitigung eingegrenzt, deren Art und Umfang sich nach Treu und Glauben bestimmen.[6] Aus der bisherigen Rechtsprechung des BGH lässt sich ableiten, dass ein ganz wesentliches Element in der Abwägung darin besteht, ob der Anspruchsgegner einen wirtschaftlichen Vorteil aus der Rechtsverletzung durch den Dritten zieht.[7]

Bei WLAN-Hotspot-Betreibern ist zu berücksichtigen, dass diese lediglich ein automatisch ablaufendes Verfahren zur Verfügung stellen, welches ihren Kunden den Zugriff auf die Internetinhalte vermittelt und sie auch keinen wirtschaftlichen Vorteil aus der Rechtsverletzung durch den Dritten ziehen. Ihr passiv neutraler automatischer Beitrag ist nicht vergleichbar mit dem eines Plattformbetreibers, wie er den BGH-Entscheidungen zu den Internetauktionshäusern zu Grunde lag,[8] und dem eines Forenbetreibers. Dort hat bei der Frage der Zumutbarkeit von Pflichten darauf abgestellt werden können, dass die Betreiber der Plattformen und Foren selbst die Gefahrenquellen für Rechtsverletzungen gesetzt haben, es ihnen gerade

[5] Seit dem Urteil *„Internetversteigerung I",* GRUR 2004, 860 bestätigt und auf den vorbeugenden Unterlassungsanspruch erweitert durch das Urteil *„Internetversteigerung II"*, GRUR 2007, 708 erweitert auch auf Forenbetreiber durch das Urteil „Meinungsforum", GRUR 2007, 724; BGH, GRUR 2008, 702, 705, Rn. 38 – *Internet-Versteigerung III.*

[6] vgl. zu zumutbaren Vorkehrungsmaßnahmen: BGH, GRUR 1984, 54, 55 – *Kopierläden*; vgl. zu zumutbaren Prüfpflichten: BGH, GRUR 1999, 418, 420 – *Möbelklassiker* und GRUR 1997, 313, 315 – *Architektenwettbewerb.*

[7] BGH, MMR 2004, 668, 671 - *Internetversteigerung I*; BGH NJW 2007, 890 – *Jugendgefährdende Medien bei eBay*; OLG München MMR 2006, 739, 740; OLG Hamburg, MMR 2006, 744, 745.

[8] So auch OLG Frankfurt a.M., GRUR-RR 2008, 93, 94 – *Access-Provider*, dort zu wettbewerbsrechtlichen Ansprüchen.

auch auf die Inhalte ankommt und dass dort ganz andere Möglichkeiten einer besseren Beeinflussung und Kontrolle der Inhalte besteht. WLAN-Hotspot-Betreiber setzen demgegenüber selbst keine neue Gefahrenquelle und haben als neutraler technischer Vermittler mit den von ihnen vermittelten Inhalten nichts zu tun und keinerlei Einfluss darauf. Sie haben damit einen deutlich größeren Abstand zu den rechtsverletzenden Inhalten, wodurch auch die Zumutbarkeitsgrenzen eingeengt werden müssen.

Die in Frage kommenden Maßnahmen der Filterung des Datenverkehrs, einer URL-Sperre durch Verwendung eines Zwangs-Proxys, einer IP-Sperre und einer DNS-Sperre sind technisch möglich, aber so leicht zu umgehen, dass sie als wirkungslos eingestuft werden können.[9] Auch wenn eine Prüfungspflicht bejaht wird, sind zudem nur Sperrmaßnahmen zumutbar, die automatisiert mit entsprechender Filtersoftware durchführbar sind.[10] Wenn die Rechtsprechung von WLAN-Hotspot-Betreibern aber etwa verlangen würde, den Zugang zu einem Internetauftritt zu sperren, weil ihre Kunden beim Aufruf dieser Seite eine Rechtsverletzung begehen (könnten), dann bedürfte es einer umfassenden Prüfung in sachlicher und rechtlicher Hinsicht, ob die jeweilige Sperrung tatsächlich gerechtfertigt ist. Das bedingt eine zeitlich durchaus aufwendige auch juristische Prüfung. Weiter müsste die geforderte Sperre eingerichtet und gegebenenfalls kontrolliert werden. Insgesamt wird für die Erfüllung dieser Aufgaben eine neue Infrastruktur erforderlich sein. Der damit verbundene Aufwand und der potentielle Nutzen sind bei der Zumutbarkeitsprüfung zu berücksichtigen.

Im Rahmen der Verhältnismäßigkeit wird man von den WLAN-Hotspot-Betreibern unter Berücksichtigung des dargestellten zusätzlichen Aufwandes letztlich um so weniger die Einrichtung von derartigen Sperren verlangen können, je geringer die Eignung ist, dass Ziel der Verhinderung von Urheberrechtsverstößen zu erreichen. Das LG Hamburg sagt dazu etwa:

> *„Ohne Erfolg verweisen die Ast. darauf, dass die Mehrzahl der durchschnittlichen Internetnutzer durch eine DNS-Sperre davon abgehalten würden, einen anderen Weg zu dem gesperrten Internetauftritt zu suchen. Dem Gericht ist es in wenigen Minuten*

[9] LG Hamburg, Urteil vom 12.03.2010 - 308 0 640/08, nicht rechtskräftig, MMR 2010, 488, 489.
[10] *Leistner/Stang,* WRP 2008, 546; *Ingerl/Rohnke*, Markengesetz, 3. Auflage 2010, Nach § 15, Rn. 222.

gelungen, eine Internetseite mit einer Anleitung zur Umgehung mit den verfügbaren Nameservern zu finden. Den Nutzern solcher Filmdownloadseiten wie „…in", es dürften im Wesentlichen internetaktive Jugendliche und junge Erwachsene sein, wird das im Zweifel noch schneller gelingen."[11]

Insgesamt ist unter Berücksichtigung der eingeschränkten Wirkung denkbarer Filesharing-„Sperren", der durch die rein objektive Unterstützung von möglichen Verletzungshandlungen durch WLAN-Hotspot-Nutzer eingeschränkten bzw. fehlenden Zumutbarkeit und des Prüfungsaufwands auch unter Berücksichtigung der Interessen der Rechteinhaber ein Unterlassungsanspruch aus Störerhaftung m.E. zu verneinen. Denn je leichter eine Erschwerungsmaßnahme umgangen werden kann, desto weniger wird von WLAN-Hotspot-Betreibern die Einrichtung einer solchen Sperre verlangt werden können.[12]

Für Erstaunen hat vor diesem Hintergrund ein – ohne mündliche Verhandlung ergangener – Beschluss des LG Hamburg vom 25.11.2010 (Az: 310 O 433/10)[13] gesorgt, in welchem die 10. Kammer des Gerichts entschieden hat, dass der Betreiber eines Internet-Cafés nach den Grundsätzen der Störerhaftung verschuldensunabhängig auf Unterlassung wegen (Urheber-) Rechtsverletzungen die durch einen Kunden begangen wurden haften kann, wenn er keine ihm möglichen und zumutbaren Maßnahmen ergreift, um solche Rechtsverletzungen zu verhindern. Was die 10. Kammer damit meint, bleibt unklar. Wenn angesprochen sein sollte, dass der WLAN-Betreiber seine Kunden auf die Einhaltung der gesetzlichen Vorgaben hingewiesen haben muss, um einer Haftung zu entgehen, wäre dies unproblematisch.

Zu begrüßen ist insoweit ein Urteil des LG Frankfurt am Main vom 18.08.2010 (Az: 2-6 S 19/09),[14] wonach Hotels und damit letztlich auch

[11] LG Hamburg, Urteil vom 12. 11. 2008 - 308 O 548/08 (nicht rechtskräftig), NJOZ 2010, 443ff.
[12] LG Hamburg, Urteil vom 12.03.2010 - 308 0 640/08, nicht rechtskräftig, MMR 2010, 488, 490.
[13] Veröffentlicht u.a. in MIR 01/2011 unter http://medien-internet-und-recht.de/pdf/VT-MIR-2011-Dok-005.pdf; dazu *Jaeschke*, http://www.hotelier.de/news/2011/38036/Wie-haften-Hotels-Gaststaetten-oder-Internetcafes-fuer-Urheberrechtsverletzungen-durch-Filesharing.
[14] LG Frankfurt am Main, Urteil vom 18.08.2010, Az: 2-6 S 19/09; abrufbar unter www.ipjaeschke.de ; Vorinstanz: AG Frankfurt am Main, Urteil vom 25.09.2009, Az. 31 C 266/08-16

andere Access-Provider nicht für das unerlaubte Filesharing von Gästen haften:

> *„Eine Haftung des Klägers als Täter oder Teilnehmer kommt schon deshalb nicht in Betracht, weil unstreitig weder der Kläger noch dessen Angestellte ein Werk der Beklagten auf einem Computer zum Abruf durch andere Teilnehmer einer Tauschbörse bereitgestellt und damit der Öffentlichkeit zugänglich gemacht noch solches unterstützt haben. Auch eine Haftung des Klägers als Störer kommt vorliegend nicht in Betracht. Hinsichtlich seiner Gäste, denen er den Zugang zu dem verschlüsselten Funknetzwerk vermittelt hat, ergibt sich dies daraus, dass er diese zuvor auf die Einhaltung der gesetzlichen Vorgaben hingewiesen hat. Eine weitergehende Prüfungspflicht vor einer ersten Rechtsverletzung besteht für den Kläger - unabhängig von der Frage, ob sein Geschäftsmodell durch die Auferlegung präventiver Prüfungspflichten nicht ohnehin gefährdet wäre (vgl. BGHZ 158, 236, 251f.) - auf Grund der Verschlüsselung nicht (BGH GRUR 2010, 633, 635; OLG Frankfurt am Main GRUR-RR 2008, 279ff.). Hinsichtlich Dritter ergibt sich dies ebenfalls auf Grund der einstreitig erfolgten marktüblichen Verschlüsselung des Funk-Netzwerkes mit dem dieses ausreichend (BGH GRUR 2010, 633, 635) gegen Urheberrechtsverletzungen durch Dritte gesichert war“*[15] (Hervorhebungen nicht im Original).

Eine höchstrichterliche Entscheidung solcher Sachverhalte durch den BGH steht jedoch noch aus. Es kann nicht mit Sicherheit vorausgesagt werden, welche Erwägungen der BGH konkret zugrunde legen würde.

Die neue Rechtsprechung des Europäischen Gerichtshofes (EuGH) wirft indes die Frage auf, ob das Konstrukt des BGH weiterhin haltbar ist oder ob es aufgrund europarechtlicher Vorgaben nicht vielmehr geboten erscheint, die Vorschriften der §§ 8-10 TMG ohne Einschränkung auch auf Unterlassungsansprüche anzuwenden.

Mit Urteilen vom 23.03.2010 hat der EuGH zu einer für die Internet- und Suchmaschinenwerbung zentralen Streitfrage Stellung genommen, nämlich ob und inwieweit durch das Werbeprogramm „AdWords“ des

[15] Dazu *Jaeschke*, http://www.hotelier.de/news/hotellerie/hotelgewerbe/38201/Frankfurt-Hotels-haftet-nicht-fuer-Urheberrechtsverletzungen-durch-Filesharing-von-Gaesten-und-kann-zudem-Erstattung-der-eigenen-Rechtsanwaltskosten-verlangen

Suchmaschinenanbieters Google Markenrechte Dritter verletzt werden können.[16] Der EuGH geht im Zuge dieser Entscheidungen auch der Frage nach, ob Google selbst die Markenrechte Dritter verletzt. Nachdem er eine eigene Markenverletzung von Google verneint, prüft der EuGH, ob Google für eine Rechtsverletzung durch seine Werbekunden verantwortlich gemacht werden kann und hält dies grundsätzlich für denkbar. Übertragen auf deutsches Recht ist damit die Frage der Störerhaftung oder einer deliktischen Haftung wegen Verletzung von Verkehrspflichten angesprochen. Der EuGH erörtert in seiner Entscheidung, ob sich Google für seinen Dienst „AdWords" auf die Haftungsprivilegierung nach Art. 14 der Richtline 2000/31/EG („E-Commerce-Richtlinie", im Folgenden: ECRL) eines Host-Providers berufen kann. Der EuGH ist insoweit zunächst der Ansicht, dass Google AdWords als Dienst der Informationsgesellschaft im Sinne der Richtlinie anzusehen ist. Die Anwendung der Haftungsprivilegierung der ECRL hält der EuGH ausdrücklich für möglich.[17] Nach Ansicht des EuGH in der google Adwords-Entscheidung darf bei Diensteanbietern, die die Kriterien der Art. 12-15 der Richtlinie erfüllen, keine Verantwortlichkeit für eine Rechtsverletzung Dritter festgestellt werden.[18] Die Rechtsprechung des EuGH kann dahin gehend verstanden werden, dass die Verantwortlichkeitsprivilegierungen der Richtlinie umfassend gelten sollen und damit, entgegen der Rechtsprechung des BGH, auch Unterlassungsansprüche einschließen.[19]

Die diesbezügliche Einschränkung, die der BGH in seiner Rechtsprechung vornimmt, lässt die Entscheidung des EuGH jedenfalls nicht erkennen.

Auch der BGH hat in seiner Entscheidung zu den Google-Vorschaubildern am 29.04.2010 in einem Obiter Dictum unter Verweis auf die Adwords-Entscheidung des EuGH darauf hingewiesen, dass sich Suchmaschinen-Betreiber grundsätzlich auf die Haftungsbeschränkung des Art. 14 ECRL berufen können, welche die Haftung vor Kenntnis von der Rechtsverletzung ausschließe.[20] Auf die Frage der Haftung gewerblicher WLAN-Hotspot-Betreiber für Urheberrechtsverletzungen durch Hotspot-Nutzer lässt sich diese Suchmaschinen-Rechtsprechung des BGH jedoch m.E. nicht exakt übertragen, denn Suchmaschinenbetreiber oder Internetversteigerungsportale können Rechtsverletzungen auf ihren eigenen Seiten nach einem konkreten Hinweis von Rechteinhabern

[16] EuGH, Urt. v. 23.03.2010 - C-236/08 u.a., GRUR 2010, 445ff.
[17] EuGH, Urt. v. 23.03.2010 - C-236/08 u.a., GRUR 2010, 445ff., Rnn. 109, 113.
[18] EuGH, GRUR 2010, 445, Rn. 107.
[19] So richtig *Stadler*, AnwZert ITR 21/2010, Anm. 2.
[20] BGH, GRUR 2010, 628, 633.

abstellen, WLAN-Hotspotbetreiber haben diese Möglichkeit nicht, denn technisch nicht leicht zu umgehende Filesharing-Sperren existieren nicht und die konkrete Überwachung des Internetnutzungsverhaltens ist weder rechtlich zulässig, noch gesellschaftlich wünschenswert oder wirtschaftlich zumutbar. Gegen gewerbliche WLAN-Hotspot-Betreiber sollte Rechteinhabern daher nicht nur kein Unterlassungsanspruch zugestanden werden, sondern die Rechtsprechung sollte auch keine Haftung des gewerblichen WLAN-Hotspot-Betreibers ab Kenntnis von einer Rechtsverletzung festschreiben.

Diese Einschätzung steht auch im Einklang mit Erwägungsgrund 46 der Richtlinie über den elektronischen Geschäftsverkehr (ECRL),[21] wo es heißt:

> *„Um eine Beschränkung der Verantwortlichkeit in Anspruch nehmen zu können, muß der Anbieter eines Dienstes der Informationsgesellschaft, der in der Speicherung von Information* (Anm.: Hervorhebung nicht im Original) *besteht, unverzüglich tätig werden, sobald ihm rechtswidrige Tätigkeiten bekannt oder bewußt werden, um die betreffende Information zu entfernen oder den Zugang zu ihr zu sperren. Im Zusammenhang mit der Entfernung oder der Sperrung des Zugangs hat er den Grundsatz der freien Meinungsäußerung und die hierzu auf einzelstaatlicher Ebene festgelegten Verfahren zu beachten. Diese Richtlinie läßt die Möglichkeit der Mitgliedstaaten unberührt, spezifische Anforderungen vorzuschreiben, die vor der Entfernung von Informationen oder der Sperrung des Zugangs unverzüglich zu erfüllen sind.“*

Gewerbliche WLAN-Hotspot-Betreiber speichern jedoch gerade keine Informationen, sondern vermitteln nur rein technisch den Zugang zu gespeicherten Informationen.

Würde der BGH seine restriktive Rechtsprechung weiterverfolgen, führte dies dazu, dass die Privilegierungstatbestände im Bereich des Zivilrechts praktisch auch in Zukunft insoweit leerlaufen, nachdem die überwiegende Zahl der Rechtsstreitigkeiten auf Unterlassung gerichtet ist. Dieses Ergebnis entspräche erkennbar nicht mehr dem Sinn und Zweck der E-

[21] Richtlinie 2000/31/EG über den elektronischen Geschäftsverkehr, ABl. Nr. L 178 S. 1, EU-Dok.-Nr. 3 2000 L 0031.

Commerce-Richtlinie. Erstaunlich ist, dass es der BGH nicht für notwendig befunden hat, die Frage dem EuGH vorzulegen.[22]

Kommerziell betriebene WLAN-Zugänge waren wie erwähnt bisher noch nicht Gegenstand der BGH-Rechtsprechung zu unerlaubtem Filesharing. Es ist jedoch aus genannten Gründen gut möglich, dass der BGH bei gewerblichen offenen WLAN-Anschlüssen zukünftig in diesen Fällen auch eine Anwendung von § 8 TMG auf Unterlassungsansprüche bejahen wird. In seinem Urteil vom 12.05.2010,[23] das einen privaten WLAN-Betreiber betraf, führt der BGH aus:

> *„Die dem privaten WLAN-Anschlussinhaberobliegende Prüfungspflicht besteht nicht erst, nachdem es durch die unbefugte Nutzung seines Anschlusses zu einer ersten Rechtsverletzung Dritter gekommen und diese ihm bekannt geworden ist. Sie besteht vielmehr bereits ab Inbetriebnahme des Anschlusses. Die Gründe, die den Senat in den Fällen der Internetversteigerung dazu bewogen haben, eine Störerhaftung des Plattformbetreibers erst anzunehmen, nachdem er von einer ersten Rechtsverletzung Kenntnis erlangt hat, liegen bei privaten WLAN-Anschlussbetreibern nicht vor. Es geht hier nicht um ein Geschäftsmodell, das durch die Auferlegung präventiver Prüfungspflichten gefährdet wäre (vgl. BGHZ 158, 236 [251f.] = NJW 2004, 3102 = GRUR 2004, 860–Internet-Versteigerung I,* Hervorhebung nicht im Original*).“*

Der BGH möchte also das Geschäftsmodell kommerzieller Betreiber vor einer Gefährdung durch präventive Prüfungspflichten schützen.

III. Kenntnisnahmeverbot aus Art. 10 GG und § 88 TKG (Fernmeldegeheimnis)

Selbst wenn man eine Anwendung von § 8 TMG auf Unterlassungsansprüche verneint, scheitert eine Haftung kommerzieller WLAN-Betreiber jedoch regelmäßig an der tatsächlichen und rechtlichen Unmöglichkeit der Verhinderung weiterer Verstöße.

[22] *Stadler*, AnwZert ITR 21/2010, Anm. 2.
[23] BGH NJW 2010, 2061.

Sinnvoll ist es insoweit, Kunden und Mitarbeitern ein, ggf. zeitlich begrenztes und ausreichend sicheres, Passwort („Ticket“) zuzuteilen, um unbefugten Dritten möglichst keinen Zugriff zu ermöglichen. Ein solches personenbezogenes Kundenpasswort hat zudem mutmaßlich den psychologischen Effekt, dass rechtsunkundige Nutzer über „ihr“ Passwort keine Rechtsverletzungen begehen werden. Eine Kennungsvergabe an die Benutzer zu dem Zweck, die Benutzer auch zu überwachen ist jedoch aufgrund von Art. 10 GG und § 88 TKG (Fernmeldegeheimnis) unzulässig.

Der Schutz des Art. 10 Abs. 1 GG[24] erfasst jegliche Art und Form von Telekommunikation. Der Schutzbereich erstreckt sich auf die Kommunikationsdienste des Internet. Soweit Art. 10 Abs. 1 GG unmittelbar nur vor staatlichen Eingriffen schützt,[25] ergibt sich daraus aber auch ein Schutzauftrag des Staates gegenüber Grundrechtsträgern, die als Private Zugriffsmöglichkeiten auf die Telekommunikation haben. Dabei ist § 88 TKG als einfachgesetzliche Ausprägung des Fernmeldegeheimnisses anzusehen[26] mit dem Ziel, die Teilnehmer der Fernkommunikation vor Kenntnisnahme und Unterdrückung durch die Anbieter der Telekommunikation zu schützen.[27] Nach § 88 Abs. 3 Satz 1 besteht ein striktes Kenntnisnahmeverbot. Danach schützt das Fernmeldegeheimnis den Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikations-Vorgang beteiligt ist oder war, und es erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.[28] Nach § 88 Abs. 3 TKG ist es WLAN-Betreibern ausdrücklich untersagt, sich Kenntnisse von Inhalt der Kommunikation zu verschaffen, wenn das nicht für den Betrieb des Netzes erforderlich ist. Als Inhalt ist grundsätzlich alles geschützt, was während des jeweiligen Telekommunikationsvorgangs ausgesandt, übermittelt oder empfangen wird. Der Schutz ist technologieneutral und umfasst auch die Kommunikation durch Computer oder sonstige Endeinrichtungen. Adressat der Schutzvorschriften ist gerade auch der Accessprovider als Anbieter i.S.d.

[24] Art. 10 [Brief-, Post- und Fernmeldegeheimnis] lautet: *„(1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich. (2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, daß sie dem Betroffenen nicht mitgeteilt wird und daß an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt.“*
[25] BVerwGE 6, 299, 300.
[26] Vgl. BT-Drs. 13/3608, S. 53, zu § 83 TKG a.F., der Vorgängerregelung zu § 88 TKG.
[27] *Schnabel*, MMR 2008, 281, 283.
[28] BVerfG, MMR 2008, 315, 316 m.w.N.

§ 3 Nr. 6 TKG.[29] Daher sind ebenfalls Nebenstellenanlagen in Betrieben, Behörden, Hotels und Krankenhäusern zur Wahrung des Fernmeldegeheimnisses verpflichtet, sobald sie ihre Telekommunikations-Anlage Dritten, z. B. auch den eigenen Mitarbeitern, zur privaten Nutzung zur Verfügung stellen.[30]

Als Sanktion bei einer Verletzung des Fernmeldegeheimnisses ist sogar die Strafbarkeit nach § 206 (Verletzung des Post- oder Fernmeldegeheimnisses) Strafgesetzbuch (StGB) vorgesehen.[31] Nach § 206 Abs. 5 StGB unterliegen dem Fernmeldegeheimnis der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche. Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Telekommunikationsdienste erbringt, wird nach § 206 Abs. 1 StGB mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft. Dies gilt nach § 206 Abs. 3 StGB u.a. auch für Personen, die von einem solchen Unternehmen oder mit dessen Ermächtigung mit dem Erbringen von Telekommunikationsdiensten betraut sind oder mit der Herstellung einer dem Betrieb eines solchen Unternehmens dienenden Anlage oder mit Arbeiten daran betraut sind.

Die Überwachung der Benutzer in Bezug auf die Verwendung von Filesharing-Programmen ist damit ausdrücklich verboten.

IV. Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Diese Sichtweise wird gestützt durch die Rechtsprechung des BVerfG und des BGH.

[29] „Diensteanbieter“ im Sinne von § 3 Nr. 6 TKG ist jeder, der ganz oder teilweise geschäftsmäßig a) Telekommunikationsdienste erbringt oder b) an der Erbringung solcher Dienste mitwirkt.
[30] Vgl. *Bock*, Beck’scher TKG-Kommentar, 3. Auflage 2006, § 88, Rn. 24; vgl. *Eckhardt*, in: Spindler/Schuster, Recht der elektronischen Medien, 1. Auflage 2008, § 88 TKG, Rnn. 10, 16ff., 22
[31] Vgl. *Bock*, Beck’scher TKG-Kommentar, 3. Auflage 2006, § 88, Rn. 61; vgl. *Eckhardt*, in: Spindler/Schuster, Recht der elektronischen Medien, 1. Auflage 2008, § 88 TKG, Rnn. 1ff.

Nach der Rechtsprechung des BVerfG umfasst das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Das allgemeine Persönlichkeitsrecht in seiner besonderen Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme tritt zu den anderen Konkretisierungen dieses Grundrechts, wie dem Recht auf informationelle Selbstbestimmung, sowie zu den Freiheitsgewährleistungen der Art. 10 und Art. 13 GG hinzu, soweit diese keinen oder keinen hinreichenden Schutz gewähren.[32]

Auch der BGH betont das Recht des Internetnutzers auf Anonymität**:**

> *„Im Hinblick auf die Anonymität der Nutzer ist eine darüber hinaus gehende Überprüfung gar nicht möglich. (…) Für Datenabfragen aus Bewertungsforen führt mithin die wortgetreue Anwendung der Vorschriften in § 29 Abs. 2 Nr. 1 a und 2 BDSG zu einem Widerspruch zu dem sich aus Art. 5 Abs. 1 GG ergebenden Recht auf uneingeschränkte Kommunikationsfreiheit. Sie ist auch nicht vereinbar mit dem bis 28. Februar 2007 in § 4 Abs. 6 Teledienstedatenschutzgesetz und seit 1. März 2007 in den §§ 12 ff. TMG gewährleisteten Recht des Internetnutzers auf Anonymität*“.[33]

V. Ergebnis

Ob der BGH bei der Beurteilung der Frage der Haftung gewerblicher WLAN-Hotspot-Betreiber für Urheberrechtsverletzungen durch Hotspot-Nutzer die Privilegierung des § 8 TMG auch auf Unterlassungsansprüche anwenden würde bzw. wird ist derzeit noch offen.

Selbst wenn man eine Anwendung von § 8 TMG auf Unterlassungsansprüche verneint, scheitert eine Haftung kommerzieller WLAN-Betreiber jedoch regelmäßig an der Unzumutbarkeit bzw. der rechtlichen Unmöglichkeit der Verhinderung weiterer Verstöße.

Sinnvoll ist es, Kunden und Mitarbeitern ein, ggf. zeitlich begrenztes und ausreichend sicheres, Passwort („Ticket“) zuzuteilen, um unbefugten Dritten

[32] Vgl. BVerfG 1 BvR 370/07, 1 BvR 595/07 (Erster Senat)**,** Urteil vom 27.02.2008.
[33] BGH, Urteil vom 23.06.2009, Az.: VI ZR 196/08 – *spickmich.de*, vgl. Vorinstanzen LG Köln, Az. 28 O 319/07; OLG Köln, Az. 15 U 43/08.

möglichst keinen Zugriff zu ermöglichen. Ein solches personenbezogenes Kundenpasswort hat zudem mutmaßlich den psychologischen Effekt, dass rechtsunkundige Nutzer über „ihr“ Passwort keine Rechtsverletzungen begehen werden. Eine Kennungsvergabe an die Benutzer zu dem Zweck, die Benutzer auch zu überwachen ist jedoch aufgrund von Art. 10 GG und § 88 TKG (Fernmeldegeheimnis) unzulässig.

Es ist zu erwarten, dass auch der BGH bei einer Beurteilung zu diesem Ergebnis kommen könnte, obgleich dies nicht mit Sicherheit vorausgesagt werden kann. Es ist demnach möglich, dass abmahnende Kanzleien klageweise gegen die Betreiber von gewerblichen WLAN-Netzen vorgehen und diese instanzgerichtlich unterliegen, obgleich es gute Argumente für die Privilegierung gewerblicher WLAN-Anbieter bzw. einen Haftungsausschluss in Bezug auf sie gibt, welchen auch ein Instanzgericht sich mutmaßlich nicht zwingend verschließen würde. Zu begrüßen ist insoweit das erwähnte Urteil des LG Frankfurt am Main vom 18.08.2010,[34] wonach Hotels und damit letztlich auch andere Access-Provider nicht für das unerlaubte Filesharing von Gästen haften.[35]

Die vorstehenden allgemeinen Ausführungen ersetzen nicht die Rechtsberatung im konkreten Einzelfall.

Gießen, den 21.02.2011

Dr. Lars Jaeschke, LL.M.
Rechtsanwalt
Fachanwalt für Gewerblichen Rechtsschutz

JAESCHKE
MARKEN- UND MEDIENRECHT

Gießen
Wilhelm-Liebknecht-Str. 35
35396 Gießen
Telefon 0641 / 68 68 1160

Frankfurt am Main
Westhafen-Tower
60327 Frankfurt am Main
Telefon 069 / 710 456 541

Telefax-Zentrale 0641 / 68 68 1161
E-Mail: jaeschke@ipjaeschke.de
www.ipjaeschke.de

[34] LG Frankfurt am Main, Urteil vom 18.08.2010, Az: 2-6 S 19/09; abrufbar unter www.ipjaeschke.de ; Vorinstanz: AG Frankfurt am Main, Urteil vom 25.09.2009, Az. 31 C 266/08-16

[35] Dazu *Jaeschke*, http://www.hotelier.de/news/hotellerie/hotelgewerbe/38201/Frankfurt-Hotels-haftet-nicht-fuer-Urheberrechtsverletzungen-durch-Filesharing-von-Gaesten-und-kann-zudem-Erstattung-der-eigenen-Rechtsanwaltskosten-verlangen.

Konkrete Handlungsmöglichkeiten für gewerbliche WLAN-Hotspot-Betreiber nach Erhalt einer Abmahnung wegen Urheberrechtsverletzung

Die folgenden Hinweise können die rechtliche Beurteilung im konkreten Einzelfall nicht ersetzen, sondern dienen der allgemeinen Information.

Nach Erhalt einer urheberrechtlichen Abmahnung ist derzeit folgendes zu raten:

1. Vorgefertigte Unterlassungsverpflichtungserklärung nicht voreilig unterschreiben

Die von den Abmahnanwälten der Abmahnung beigefügte Unterlassungsverpflichtungserklärung sollte nie voreilig unterschrieben werden, weil damit ein rechtsgültiger Vertrag geschlossen wird. Die vorgefertigten Unterlassungsverpflichtungserklärungen sind in der Regel deutlich rechteinhaberfreundlich ausgestaltet, d.h. sehr weitgehend und enthalten oft konkrete und hohe Vertragsstrafen, zu denen sich der Abgemahnte nicht verpflichten muss.

2. Fristen und weiteres Vorgehen

Innerhalb der von den Abmahnanwälten gesetzten kurzen Frist ist zu entscheiden, wie weiter vorgegangen werden soll. Für gewerbliche WLAN-Hotspot-Betreiber sind aufgrund der aktuellen Rechtsprechungstendenzen zwei Reaktionsmöglichkeiten naheliegend, die ein unterschiedliches Prozesskostenrisiko beinhalten:

a.) Abgabe einer modifizierten Unterlassungserklärung, keine Zahlung

Das abgemahnte Unternehmen gibt fachanwaltlich beraten und auf den konkreten Sachverhalt zugeschnitten eine modifizierte Unterlassungserklärung ab und verweigert die Erstattung der Abmahngebühren mit Hinweis auf Argumente für die Privilegierung gewerblicher WLAN-Anbieter und das Fernmeldegeheimnis.

Das hätte den Vorteil, dass der größte Teil des Streitwertes, nämlich der des geltend gemachten Unterlassungsanspruches, der beim Filesharing etwa vollständiger aktueller Musikalben oder Kinofilmen nicht selten zwischen € 40.000,00 - € 50.000,00 oder höher liegt, in einem möglichen Prozess wegfallen würde und Streitwert also nur noch die Abmahngebühren und etwaiger Schadensersatz wären. Erfolgt nach Abgabe einer solchen Unterlassungserklärung nochmals ein Verstoss gegen die Urheberrechte des abmahnenden Rechteinhabers müsste das abgemahnte Unternehmen allerdings eine Vertragsstrafe zahlen, deren Höhe letztlich ein Gericht festlegen würde. Aus diesem Grund ist auch die Abgabe einer Vielzahl sog. vorbeugender Unterlassungserklärungen bei gewerblichen WLAN-Anbietern im Regelfall keinesfalls zu empfehlen. Eine einzelne modifizierte Unterlassungserklärung gilt nicht gegenüber anderen Rechteinhabern. Oft ist diese Variante zu empfehlen, da die Abgabe einer Unterlassungserklärung ohne Anerkennung einer Rechtspflicht in solchen Konstellationen aufgrund des viel geringeren Streitwertes das Prozesskostenrisiko und aufgrund der unklaren Rechtslage das Risiko, überhaupt verklagt zu werden, deutlich senkt.

b.) Keine Abgabe einer Unterlassungserklärung, keine Zahlung

Alternativ könnte nicht nur die Zahlung der Abmahngebühren, sondern auch die Abgabe einer modifizierten Unterlassungserklärung mit Hinweis auf Argumente für die Privilegierung gewerblicher WLAN-Anbieter und das Fernmeldegeheimnis verweigert werden. Je nach vom Gericht angesetzten Streitwert (abhängig vom Werk sind € 10.000,00 (einzelnes Lied) oder auch € 50.000,00 (aktuelles Musikalbum aus den Charts) Streitwert allein für den Unterlassungsanspruch nach Ansicht einiger Gerichte nicht zu hoch angesetzt und bei Urheberrechtsverletzungen im Internet

kann sich die Gegenseite vereinfacht gesagt einen Gerichtsstand aussuchen) müsste mit einem Prozesskostenrisiko von vielen tausend Euro schon in der ersten Instanz gerechnet werden.

Ohne Abgabe einer modifizierten Unterlassungserklärung kann zudem gesondert vom Weg der sog. Hauptsacheklage ein einstweiliges Verfügungsverfahren angestrengt werden, bei welchem gesonderte Kosten aus dem Streitwert entstehen, welche von der unterliegenden Partei zu tragen sind.

Da die Frage der Haftung gewerblicher WLAN-Hotspot-Betreiber für Urheberrechtsverletzungen durch Hotspot-Nutzer noch nicht höchstrichterlich entschieden ist, würde der Rechtsstreit möglicherweise über mehrere Instanzen gehen, wobei der Ausgang letztlich noch offen ist.

Welche Reaktionsmöglichkeit angezeigt ist, sollte von Fall zu Fall nach Absprache mit einem Fachanwalt für Gewerblichen Rechtsschutz festgelegt werden. Jedenfalls die Zahlung der geltend gemachten Abmahngebühren vollumfänglich zu verweigern erscheint vor dem Hintergrund der aktuellen Rechtsprechungstendenzen regelmäßig vertretbar.

c.) Netzwerk gegen unbefugte Dritte absichern („WPA 2“ und Passwort)

In allen Fällen sollte das WLAN-Netz zumindest zukünftig nicht völlig ungesichert sein, sondern jedenfalls mit dem bei Einrichtung aktuellen Sicherheitsstand versehen werden (derzeit WPA 2 – Verschlüsselung), wobei Kunden und Mitarbeitern ein, ggf. zeitlich begrenztes und ausreichend sicheres, Passwort zugeteilt werden sollte, um unbefugten Dritten möglichst keinen Zugriff zu ermöglichen. Ein solches personenbezogenes Kundenpasswort hat zudem mutmaßlich den psychologischen Effekt, dass rechtsunkundige Nutzer über „ihr“ Passwort keine Rechtsverletzungen begehen werden. Wie umfangreich verkehrsübliche Sicherungsmaßnahmen im gewerblichen Verkehr konkret sein müssen, um die Haftung von Betreibern gewerblicher WLAN-Netze im Falle unerlaubten Filesharings durch Dritte auszuschliessen, ist noch ungeklärt. In der aktuellen Entscheidung *„Sommer unseres*

Lebens“, die Filesharing im Privatbereich betrifft, hat der BGH aber jedenfalls entschieden:

> *„Das hoch zu bewertende, berechtigte Interesse, über WLAN leicht und räumlich flexibel Zugang zum Internet zu erhalten, wird nicht dadurch in Frage gestellt, dass die zum Zeitpunkt der Installation des WLAN-Routers auch* (Anm.: Hervorhebung nicht im Original) *im Privatbereich verkehrsüblich vorhandenen Sicherungsmaßnahmen gegen unbefugte Nutzung angewandt werden.“*

Ein völlig ungesichertes WLAN-Netz kann nach derzeitiger Rechtslage keinesfalls empfohlen werden.

d.) Regelung in Arbeitsverträgen bzw. Internetnutzungsbedingungen

Keinesfalls sollte auch das Internetsurf- bzw. Downloadverhalten von Kunden und/oder Mitarbeitern überwacht und gegen das Fernmeldegeheimnis verstoßen werden, da dies strafrechtliche Konsequenzen nach sich ziehen müsste.

Es sollte jedoch in Arbeitsverträgen der Mitarbeiter bzw. in den Internetnutzungsbedingungen gegenüber Kunden („WLAN-Hotspot-AGB“), denen die Internetnutzung ermöglicht wird, klargestellt werden, dass keine urheberrechtlich geschützten Werke heruntergeladen werden dürfen oder anderweitig gegen geltendes Recht verstoßen werden darf, denn mit Urteil vom 18.08.2010 (Az: 2-6 S 19/09; abrufbar unter www.ipjaeschke.de) hat das LG Frankfurt am Main entschieden, dass Hotels und damit letztlich auch andere Access-Provider nicht für das unerlaubte Filesharing von Gästen haften, wenn eine marktübliche Verschlüsselung vorgenommen wurde und die Gäste auf die Einhaltung geltenden Rechts hingewiesen wurden. Mit Urteil vom 04.10.2007 hatte schon das LG München I (Az.: 7 O 2827/07) entschieden, dass ein Arbeitgeber grundsätzlich nicht für die illegale Teilnahme eines Mitarbeiters an einem Filesharing-System haftet, wenn der Arbeitnehmer auf das Verbot illegalen Filesharings hingewiesen wurde. In dem dort entschiedenen Fall hatte der Mitarbeiter 1394 Audio-Dateien illegal

heruntergeladen. Das Landgericht hat geurteilt, dass der Mitarbeiter rein privat und entgegen seiner arbeitsvertraglichen Verpflichtungen gehandelt habe. Der Arbeitgeber habe nicht gegen die im Verkehr erforderliche Sorgfalt verstossen, da keine Lebenserfahrung dahingehend existiere, dass Mitarbeiter bereitgestellte Computer per se für Urheberrechtsverletzungen nutzten. Obgleich die Entscheidung schon aus dem Jahr 2007 stammt, ist auch sie ein Anhaltspunkt dafür, welche Maßnahmen gewerblichen WLAN-Betreibern zur Verhinderung von Urheberrechtsverstößen durch Mitarbeiter, Kunden und sonstige Dritte allenfalls zumutbar sind.

Die vorgenannten allgemeinen Hinweise können nie die rechtliche Beurteilung im konkreten Einzelfall ersetzen.

Gießen, den 21.02.2011

Dr. Lars Jaeschke, LL.M.
Rechtsanwalt
Fachanwalt für Gewerblichen Rechtsschutz

JAESCHKE
MARKEN- UND MEDIENRECHT

Gießen
Wilhelm-Liebknecht-Str. 35
35396 Gießen
Telefon 0641 / 68 68 1160

Frankfurt am Main
Westhafen-Tower
60327 Frankfurt am Main
Telefon 069 / 710 456 541

Telefax-Zentrale 0641 / 68 68 1161
E-Mail: jaeschke@ipjaeschke.de
www.ipjaeschke.de

Die nachstehenden Muster-AGB sind mit größter Sorgfalt erstellt, erheben jedoch keinen Anspruch auf Vollständigkeit und Richtigkeit. Ein Haftungsanspruch aufgrund der Verwendung der Muster-AGB durch Kunden der LANCOM Systems GmbH gegenüber der LANCOM Systems GmbH ist ausgeschlossen.

Allgemeine Nutzungsbedingungen WLAN-Hotspot

I. Vertragspartner

Vertragspartner sind die *„Musterunternehmen, Musterstr. 0, 12345 Musterstadt“* (im Folgenden „Hotspot-Betreiber“ genannt) und der Gast/Kunde als WLAN-Nutzer (im Folgenden „Kunde“ genannt).

II. Vertragszweck

Die Aufgabe des Hotspots besteht darin, Kunden einen einfachen Zugang zum Internet zu ermöglichen und dafür die erforderliche Freischaltung der Kunden durchzuführen. Die vorliegenden Nutzungsbedingungen regeln (in Verbindung mit dem Telekommunikationsgesetz – TKG) die Inanspruchnahme des Hotspots des Hotspot-Betreibers durch den Kunden.

III. Zustandekommen des Hotspot-Nutzungsvertrages

Der Vertrag bezüglich der Hotspot-Nutzung zwischen dem Hotspot-Betreiber und dem Kunden kommt dadurch zustande, dass der Kunde seinen Benutzernamen und ein Passwort (im Folgenden „Ticket“ genannt) eingibt und das Pflichtfeld *„Allgemeine Nutzungsbedingungen WLAN-Hotspot gelesen und akzeptiert“* durch Anklicken aktiviert. Erst danach ist eine Nutzung des Internet über den Hotspot für den Kunden möglich. Benutzername ist …(z.B. der Nachnahme oder die Zimmernummer des Kunden). Das Ticket erhält der Kunde auf Nachfrage beim Hotspot-Betreiber. Das Ticket ist (volumen- oder) zeitbasiert. (Der Kunde kann jederzeit durch einfaches Trennen der Verbindung zum Hotspot die aktuelle Internetsitzung unterbrechen und im Rahmen der zeitlichen Gültigkeit später fortsetzen.)

IV. Nutzungsvoraussetzungen

Die zur Nutzung des Hotspot-Dienstes erforderliche Hardware (insbesondere ein WLAN-fähiges Endgerät) und Software stellt der Kunde selbst bereit. (besondere technische Nutzungsvoraussetzungen ?)

V. Leistungen des Hotspot-Betreibers

Die Vermittlung des Internetzugangs über den Hotspot des Hotspot-Betreibers wird als Dienstleistung des Hotspot-Betreibers im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten angeboten. Zeitweilige Störungen etwa aufgrund höherer Gewalt, Wartungsmaßnahmen o.ä. können nicht ausgeschlossen werden. Der Hotspot-

Betreiber wird alle zumutbaren Anstrengungen unternehmen, um solche Störungen unverzüglich zu beseitigen bzw. auf deren Beseitigung hinzuwirken. Der Hotspot-Betreiber garantiert aus technischen Gründen keine bestimmte Übertragungsgeschwindigkeit.

VI. Haftung des Hotspot-Betreibers

Der Hotspot-Betreiber haftet dem Kunden auf Schadenersatz für vertragliche Pflichtverletzungen sowie aus Delikt nur bei Vorsatz oder grober Fahrlässigkeit des Hotspot-Betreibers, seines gesetzlichen Vertreters oder Erfüllungsgehilfe.

Dies gilt nicht bei Verletzung von Leben, Körper und Gesundheit des Kunden, Ansprüchen wegen der Verletzung von Kardinalpflichten, d.h. von Pflichten, die sich aus der Natur des Vertrages ergeben und bei deren Verletzung die Erreichung des Vertragszwecks gefährdet ist, dem Ersatz von Verzugsschäden (§ 286 BGB) sowie für die Haftung nach dem Produkthaftungsgesetz. Insoweit haftet der Hotspot-Betreiber für jeden Grad des Verschuldens.

Bei schuldhafter – weder vorsätzlicher noch grob fahrlässiger – Verletzung wesentlicher Vertragspflichten ist die Haftung begrenzt auf den Ersatz des vertragstypischen, vorhersehbaren Schadens bis zu einer Höhe von maximal 1.000,00 Euro.

Für fahrlässig verursachte Schäden aus Datenverlust ist die Haftung des Hotspot-Betreibers ausgeschlossen.

VII. Pflichten und Obliegenheiten des Kunden

1. Keine Weitergabe des Tickets

Eine Weitergabe des Tickets durch den Kunden und/oder die Nutzung des Tickets durch Dritte ist untersagt. Erlangt der Hotspot-Betreiber Kenntnis von der Weitergabe des Tickets durch den Kunden und/oder die Nutzung des Tickets durch Dritte kann der Hotspot-Betreiber das Ticket deaktivieren.

2. Datenschutz

Der nach der Anmeldung durch den Kunden vermittelte Datenverkehr zwischen dem Hotspot und dem Endgerät des Kunden wird unverschlüsselt übertragen. Es ist deshalb möglich, dass Dritte die übertragenen Daten einsehen und/oder auf diese zugreifen können. Der Kunde trägt die Verantwortung für den Schutz (z.B. durch eine geeignete Firewall, Virenschutz, regelmäßige Datensicherung etc.) und die Verschlüsselung (z.B. https, VPN) seiner Daten.

3. Missbräuchliche Nutzung des Hotspot durch den Kunden

Der Hotspot-Betreiber tritt als neutraler technischer Vermittler auf und hat auf die vermittelten Inhalte keinen Einfluss. Der Kunde ist selbst für die Internetinhalte die er über den Hotspot abruft und/oder verbreitet bzw. öffentlich zugänglich macht verantwortlich. Eine inhaltliche Überwachung durch den Hotspot-Betreiber erfolgt nicht.

Der Kunde verpflichtet sich, den Hotspot nicht missbräuchlich zu nutzen. Als missbräuchliche Nutzung des Hotspots gilt insbesondere

- die Verletzung von Urheber- und sonstigen Rechten Dritter, insbesondere die rechtsverletzende Nutzung von sog. Peer-to-Peer Netzwerken bzw. „Internettauschbörsen“ („illegales Filesharing“),
- die Verbreitung und öffentliche Zugänglichmachung von schädigenden und/oder rechtswidrigen Inhalten, einschliesslich des Versands von unverlangten Massen-E-Mails, (sog. „Spamming“) und Viren,
- das Übermitteln von sittenwidrigen, belästigenden oder anderweitig unerlaubten Inhalten, deren Einstellen in das Internet oder das Hinweisen auf solche Inhalte im Internet,
- das Eindringen in fremde Datennetze sowie der Versuch des Eindringens in fremde Datennetze (sog. „Hacking“),
- das Benutzen von Anwendungen oder Einrichtungen, die zu Störungen/Veränderungen an der physikalischen oder logischen Struktur der Hotspot-Server des Hotspot-Betreibers, des Hotspot-Netzes des Hotspot-Betreibers oder anderer Netze führen oder führen können.

4. Haftungsfreistellung seitens des Kunden

Der Kunde stellt den Hotspot-Betreiber von sämtlichen Ansprüchen Dritter frei, die auf einer rechtswidrigen Verwendung des Hotspot durch den Kunden beruhen oder mit seiner Billigung erfolgen oder die sich aus urheberrechtlichen oder sonstigen rechtlichen Streitigkeiten ergeben, die mit der Nutzung des Hotspot durch den Kunden verbunden sind. Erkennt der Kunde oder muss er erkennen, dass ein solcher Rechtsverstoss geschehen ist oder droht, hat er die Pflicht zur unverzüglichen Unterrichtung des Hotspot-Betreibers. Bei Verschulden haftet der Kunde dem Hotspot-Betreiber auf Ersatz der entstandenen Schäden.

(VIII. Entgelte für die Nutzung des Hotspot durch den Kunden

Es gilt die aktuelle Preisliste, die hier abgerufen werden kann. Es bestehen die folgenden Zahlungsmöglichkeiten: … (oder z.B.: Die Nutzung des Hotspot ist für den Kunden für die Dauer seines Aufenthaltes kostenfrei).)

IX. Sonstiges

Die vorstehenden Bestimmungen regeln das Hotspot-Nutzungsverhältnis zwischen den Hotspot-Betreiber und dem Kunden abschließend.

Mündliche Nebenabreden bestehen nicht.

Es gilt das Recht der Bundesrepublik Deutschland.