



# Das Unternehmen als Internet Access Provider

Rechtliche Aspekte des Angebots von Internetzugängen in Hotels, Cafés, Krankenhäusern, Universitäten, Flughäfen und ähnlichen Einrichtungen



*Ergebnisse eines Rechtsgutachtens im Auftrag des  
VAF Bundesverband Telekommunikation e.V.*

## Impressum

### Das Unternehmen als Internet Access Provider

Rechtliche Aspekte des Angebots von Internetzugängen in Hotels, Cafés, Krankenhäusern, Universitäten, Flughäfen und ähnlichen Einrichtungen

#### Hinweis zur 1. Auflage 2011

Das vorliegende Dokument fasst wesentliche Ergebnisse eines Rechtsgutachtens zusammen, das durch den Verfasser Rechtsanwalt Wolfgang Müller im Auftrag des VAF Bundesverband Telekommunikation erarbeitet und zum Juli 2011 fertiggestellt wurde. Der Verfasser ist Fachanwalt für Informationstechnologierecht in der Kanzlei Schlüter, Graf und Partner in Dortmund und Lehrbeauftragter der Technischen Universität Dortmund an der Fakultät für Informatik sowie Lehrbeauftragter der Fachhochschule Dortmund im Fachbereich Informatik.

#### Hinweis zur 2. Auflage 2013

Das Gutachten und diese Zusammenfassung wurden im Sommer 2013 durch den Verfasser darauf hin überprüft, ob aufgrund neuer Rechtsprechung und Gesetzgebung Korrekturbedarf zu den in der ersten Auflage getroffenen Aussagen besteht. Nach erfolgter Prüfung wird die Auffassung vertreten, dass die bereits in 2011 gefundenen Ergebnisse unverändert Anwendung finden. Die in diesem Dokument vorgelegte Zusammenfassung ist darum unverändert. Lediglich der Vollständigkeit halber wird eine - für den Betrachtungsfall „Unternehmen“ allerdings nicht maßgebliche - Klarstellung zum Bereich privater Nutzung im häuslichen Umfeld aufgenommen (Anmerkung zu Kapitel 4). Somit wird das Urteil des Bundesgerichtshofs vom 15.11.2012 mit berücksichtigt, welches auch in seiner Begründung der hier bereits vertretenen Auffassung entspricht.

#### Herausgeber

VAF Bundesverband Telekommunikation e.V.  
Otto-Hahn-Str. 16, 40721 Hilden  
[www.vaf-ev.de](http://www.vaf-ev.de)

Verantwortlicher Ansprechpartner für Publikationen des Herausgebers ist der Geschäftsführer Martin Bürstenbinder.

#### Bilder:

© iStockphoto.com / wakila | damircudic  
© Alliance | michaeljung | epstock / shutterstock.com

#### Layout:

Uwe Klenner, Layout & Gestaltung, Passau

#### Lektorat:

Stephanie Esser, [www.textschliff.de](http://www.textschliff.de)

Copyright: VAF Juni 2013, 2. überarbeitete Auflage. Erstveröffentlichung im August 2011.

Der Herausgeber hat dieses Dokument mit größter Sorgfalt erstellt, dennoch übernimmt er keine Haftung für Druckfehler, sonstige Fehler, Vollständigkeit oder Aktualität. Es wird darauf hingewiesen, dass dieser Text eine allgemeine Information darstellt. Die Verantwortung für die Nutzung dieser Informationen liegt beim Verwender. Im Einzelfall sind immer die besonderen Umstände zu würdigen.

Vervielfältigung und Veröffentlichung, auch auszugsweise, bedürfen der vorherigen schriftlichen Zustimmung des Herausgebers.

## Inhalt

1. Einleitung
2. Begriffe
3. Keine Haftung für fremde Informationen
4. Sicherheit ja, Überwachung nein
5. Enge Grenzen für Speicherung und Weitergabe von Daten
6. Abschlusskommentar
7. Praxishinweise
8. Anhang

## 1. Einleitung

Soweit Unternehmen generell oder an speziellen Orten wie z.B. die Deutsche Bahn in Bahnhöfen oder in Zügen, die Betreiber von Flughäfen, ein Hotel, ein Krankenhaus, ein Café oder eine Universität einen Internetzugang zur Verfügung stellen, nehmen diese Unternehmen, wenn sich ihr diesbezügliches Tätigwerden auf die Bereitstellung des Zugangs zum Internet beschränkt, (lediglich) die Aufgaben eines Access Providers wahr.

Access Provider stellen den jeweiligen Nutzern den Zugang zum Internet zur Verfügung, mittels dessen diese sodann Inhalte abrufen oder übertragen können.

In jüngerer Vergangenheit wurden in Fachkreisen, teils aber auch in der Presseöffentlichkeit, Fragen der Rechte und Pflichten und insbesondere der Verantwortlichkeiten des Access Providers für wettbewerbsrechtliche und urheberrechtliche Verstöße durch Nutzer, beispielsweise Gäste im Hotel oder Café, diskutiert.

Vor dem Hintergrund der gegebenen Gesetzeslage, der einschlägigen und höchst-richterlichen Rechtsprechung sowie Kommentierung in der juristischen Fachliteratur erbringt das Gutachten als wesentliches Ergebnis die Klarstellung, dass das bloße Angebot des Zugangs zum Internet keine Haftung des gewerblichen Zugangsanbieters für eventuelle Rechtsverletzungen durch Nutzer verursacht.

Dieses für Betreiber von Hotels, Cafés, Krankenhäusern usw. generell positive Ergebnis wird in der hier vorliegenden Zusammenfassung erläutert und ergänzt durch die Darstellung der maßgeblichen Rechte und Pflichten, die für das gesetzeskonforme Angebot von Internetzugängen durch ein Unternehmen zu beachten sind.

## 2. Begriffe

Wichtige begriffliche Unterscheidungen im Bereich Recht und Internet:

**Nutzer** – Derjenige, der sich Inhalte ansieht, sie abrufen oder herunterlädt – insbesondere um Informationen zu erlangen oder zugänglich zu machen –, also in irgendeiner Form Angebote nachfragt.

**Ersteller eines rechtswidrigen Zustands** – Der Ersteller oder „Urheber“ des rechtswidrigen Zustands bzw. der Rechtsverletzung, insbesondere der, der Raubkopien von Software, Filmen oder Musikstücken herstellt, persönlichkeitsverletzende Artikel oder Boykottaufrufe verfasst, unlauter wirbt oder geschützte Marken verwendet.

**Content Provider** – Der Content Provider (content = Inhalt) stellt selbst erstellte Inhalte auf eigenen Rechnern zur Verfügung. Z. B. in Form von Informationsportalen wie *spiegel.de* oder *t-online.de*. Aber auch der, der sich z. B. über Frames oder Links fremde Inhalte so zu eigen macht, dass die Inhalte nicht mehr als fremd zu erkennen sind.

**Host Provider** – Der Host Provider (host = Gastgeber) erstellt keine Inhalte, sondern speichert fremde Inhalte für einen Dritten (den Ersteller) und macht sie zugänglich.

**Access Provider** – Der Access Provider (access = Zugang) vermittelt lediglich den Zugang zu den Inhalten, die der Host oder der Content Provider speichert.

**Netz-Provider** – Der Netz-Provider steht in keinem Kontakt zu dem Nutzer. Er unterhält lediglich die Netze, über die die Kommunikation abläuft.

*(Nach Hoeren/Sieber, Handbuch Multimedia-Recht, C.H. Beck 2011)*

## 3. Keine Haftung für fremde Informationen

**Access Provider sind grundsätzlich nicht für fremde Informationen verantwortlich und dementsprechend nicht haftbar auf Schadenersatz.**

Eine Haftung eines Access Providers aus Deliktsrecht auf Schadenersatz, insbesondere gemäß § 823 BGB für Handlungen des Nutzers des Internetzugangs, käme nur in Betracht, wenn der Zugangsanbieter mit dem Nutzer bewusst und gewollt zusammenwirkt, also gemeinschaftlich mit diesem eine unerlaubte Handlung begeht. Handelt der Access Provider nicht auf solche Weise, ist eine dementsprechende Haftung regelmäßig wegen der Privilegierung gemäß § 8 TMG ausgeschlossen.

### Telemediengesetz TMG

*§ 8 Durchleitung von Informationen.*

*(1) Diensteanbieter sind für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich, sofern sie*

- 1) die Übermittlung nicht veranlasst haben,*
- 2) den Adressaten der übermittelten Informationen nicht ausgewählt und*
- 3) die übermittelten Informationen nicht ausgewählt oder verändert haben.*

*Satz 1 findet keine Anwendung, wenn der Diensteanbieter absichtlich mit einem Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen.*

*(2) Die Übermittlung von Informationen nach Absatz 1 und die Vermittlung des Zugangs zu ihnen umfasst auch die automatische kurzzeitige Zwischenspeicherung dieser Informationen, soweit dies nur zur Durchführung der Übermittlung zur Kommunikation geschieht und die Informationen nicht länger gespeichert werden, als für die Übermittlung üblicherweise erforderlich ist.*

## 4. Sicherheit ja, Überwachung nein

**Access Provider müssen ihr Zugangsnetz nach den Regeln der Technik sichern (z. B. WLAN-Verschlüsselung). Eine Verpflichtung für gewerbliche Access Provider zur Prüfung oder Überwachung, ob Nutzer den Internetzugang für rechtsmissbräuchliche Handlungen verwenden, ist jedoch zu verneinen.**

Wer als Access Provider den Zugang zum Netz nicht sichert, setzt sich dem Risiko der sogenannten Störerhaftung aus. Darunter versteht man allgemein formuliert Haftung dadurch, dass man aktiv oder passiv zu einer Rechtsgutverletzung beiträgt, ohne die erforderlichen Sicherungsmaßnahmen ergriffen zu haben. Die Einrichtung von Maßnahmen zum Schutz des Zugangsnetzes muss also als Mindestanforderung gelten. Im Falle eines WLAN-Hotspots ist dies beispielsweise die Aktivierung eines aktuellen Verschlüsselungsverfahrens.

Den sicheren Betrieb des Netzes vorausgesetzt, wird der Versuch, einen Access Provider über den Weg der »Störerhaftung« in Anspruch zu nehmen, regelmäßig an folgender Tatsache scheitern: Das einzig effektive Mittel, um entsprechende Störungen zu unterlassen bzw. von vornherein zu verhindern, würde darauf hinauslaufen, dass der Provider den Geschäftsbetrieb einstellen müsste. Die Grenze dessen, was von einem Access Provider verlangt werden kann, ist dann erreicht, wenn sein von der Rechtsordnung gebilligtes Geschäftsmodell gefährdet oder seine Tätigkeit unverhältnismäßig erschwert würde. (Urteil des Bundesgerichtshofs vom 12.07.2007)

Ebenso ist zu beachten, dass dem Access Provider umfangreiche vorbeugende Überwachungs- und Prüfpflichten wegen § 7 Abs. 2 TMG nicht auferlegt werden können:

§ 7 Abs. 2 S 1 TMG:

*(2) Diensteanbieter im Sinne der §§ 8 bis 10 sind nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. ...*

**Anmerkung:** Dieses Ergebnis ist nicht ohne Weiteres auf den Bereich eines privaten Internetzugangs zu übertragen. Zwar lehnt der BGH in seinem Urteil vom 15.11.2012 das grundsätzliche Vorliegen einer ständigen Kontrollpflicht der Internetnutzung von Minderjährigen durch die Erziehungsberechtigten ab. Allerdings muss es als durchaus zumutbar gelten, dass Minderjährige durch Eltern eingewiesen und stichprobenartig beaufsichtigt werden. Umso offensichtlicher ist, dass diese häuslichen Verhältnisse nicht auf eine gewerbliche Situation, wie in einem Hotel, Krankenhaus oder der Wartehalle eines Flughafens übertragen werden können.

## 5. Enge Grenzen für Speicherung und Weitergabe von Daten

**5. a) Die Bestimmungen zum Datenschutz und Fernmeldegeheimnis müssen beachtet werden. Der Inanspruchnahme des Access Providers auf Auskunft über Daten eines Nutzers (z. B. dynamische IP-Adresse) sind darum enge Grenzen gesetzt. Auch ein im Grundsatz u. U. zulässiger Anspruch auf Auskunft wird in der Vielzahl der Fälle ins Leere gehen müssen, da der Access Provider nicht unberechtigt Nutzerdaten vorhalten darf.**

Ein Access Provider kann dem Grundsatz nach auf Auskunft in Anspruch genommen werden. Eine derartige Auskunftsverpflichtung kann auf allgemeiner gesetzlicher Grundlage (§ 242 BGB) oder spezialgesetzlichen Regelungen (z. B. § 101 UrhG – Gesetz über Urheberrecht und verwandte Schutzrechte) beruhen. Ein Anspruch auf Auskunft setzt aber voraus, dass der Provider Auskunft geben kann und auch Auskunft

geben darf. Dies ist regelmäßig nur der Fall, wenn er berechtigterweise über die zu beauskunftenden Daten verfügt. Maßgeblich hierfür sind neben dem Bundesdatenschutzgesetz (BDSG) auch spezialgesetzliche Regelungen wie das Telemediengesetz (TMG) und das Telekommunikationsgesetz (TKG). Insbesondere die dort aufgenommenen Vorgaben zur Speicherung und zur Löschung sind penibel zu beachten. Hinzu kommt, dass das Datenschutzrecht auf dem Verbotsprinzip mit Erlaubnisvorbehalt gegründet ist, das eine Speicherung von Daten nur unter ganz engen Voraussetzungen zulässt und im Übrigen von einer Lösungsverpflichtung ausgeht. Darüber hinaus ist für den Access Provider insbesondere der § 88 TKG (Fernmeldegeheimnis) maßgeblich und zu beachten.

**5. b) Gemäß dem Urteil des Bundesverfassungsgerichts vom 2. März 2010 sind die Bestimmungen zu Speicher- und Weitergabepflichten für Daten aus § 113 a und § 113 b TKG verfassungswidrig und nichtig. Auf dieser Basis erhobene Daten waren unverzüglich zu löschen.**

Ein gesetzlicher Ausnahmetatbestand, der die ausnahmsweise Speicherung von Nutzungs-/Verkehrsdaten auf Vorrat zulässt, ist nicht gegeben. Die §§ 113 a (Speicherungspflichten für Daten) und 113 b (Verwendung der nach § 113 a gespeicherten Daten) TKG sind wegen Verstoßes gegen Artikel 10 des Grundgesetzes (Fernmeldegeheimnis) verfassungswidrig nichtig und damit unwirksam. Die auf deren Basis in der Vergangenheit gewonnenen Daten waren nach Verkündung des Urteils des Bundesverfassungsgerichts vom 2. März 2010 unverzüglich zu löschen.

**Hinweis:** Trotz dieser eindeutigen Rechtslage kann für die Praxis nicht ausgeschlossen werden, dass die – allerdings falsche – Auffassung vertreten wird, gemäß TKG bestünden ausdrückliche Pflichten zur Datenspeicherung und -weitergabe. Mögliche Quelle für solche Falschinformationen können nicht gepflegte Internetseiten sein, deren Erkenntnisstand vor dem 2. März 2010 datiert.

Somit gilt:

**1. Daten für Abrechnungszwecke:** Wenn und soweit eine Speicherung zu Abrechnungszwecken nicht notwendig ist, sind die erhobenen Nutzungs-/Verkehrsdaten unverzüglich wieder zu löschen. Hierunter fällt auch die (dynamische) IP-Adresse.

**2. Daten für technische Zwecke:** Die Speicherung von Daten für die Sicherstellung der Funktionsfähigkeit des Telekommunikationssystems ist gemäß des Urteils des Bundesgerichtshofs vom 13. Januar 2011 in einem Zeitraum von bis zu sieben Tagen noch als zulässig anzusehen. Dabei ist die Speicherung auf Daten zu beschränken, die für technische Überprüfungen, also das Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern erforderlich sind. Dazu gehören auch (dynamische) IP-Adressen.

## 6. Abschlusskommentar

Das Bundesverfassungsgericht hat dem Gesetzgeber die Schaffung einer Regelung über die Speicherung bzw. den Abruf von dynamischen IP-Adressen zum Zwecke der Verfolgung von Rechtsverstößen (insbesondere Urheberrechtsverstößen) nicht grundsätzlich untersagt. Eine entsprechende Regelung muss aber an von dem Bundesverfassungsgericht vorgegebenen Rechtsgrundsätzen anknüpfen. In der politischen Diskussion ist zurzeit insbesondere vor dem Hintergrund der Diskussion über die Vorratsdatenspeicherung als solche eine entsprechende tragfähige Gesetzesvorlage aber noch nicht erkennbar, sodass es in Bezug auf die Speicherung und Löschung bzw. Weitergabe von Daten bei dem vorstehend Ausgeführten bleibt. Vom Access Provider kann nicht mehr verlangt werden, als sich gesetzeskonform zu verhalten.

## 7. Praxishinweise

- Unternehmen wie Hotels, Krankenhäuser usw. können ihren Gästen, Patienten usw. Internetzugänge anbieten. Sie sind dann Internet Access Provider.
- Die informationstechnischen Systeme und Infrastrukturen sollten nach den aktuellen technischen Möglichkeiten sicher eingerichtet und betrieben werden. Dazu zählen etwa Authentifizierung, Verschlüsselung und technische Isolierung der Nutzer.
- Es dürfen nur die Daten erfasst werden, die für die Erfüllung des Vertrags und zu Abrechnungszwecken unbedingt erforderlich sind. Generell gilt, dass entsprechende Verkehrsdaten (z. B. auch dynamische IP-Adressen) unverzüglich gelöscht werden müssen, wenn sie nicht mehr zum Zweck der Abrechnung benötigt werden.
- Die Speicherung von Daten, die für die Sicherstellung der Funktionsfähigkeit des informations- bzw. telekommunikationstechnischen Systems erforderlich sind (z. B. auch dynamische IP-Adressen), ist in einem Zeitraum von bis zu sieben Tagen zulässig.
- Trotz der für den Access Provider grundsätzlich günstigen Rechtsposition sollte im Falle einer Abmahnung diese nicht ignoriert werden. Ein Nichtreagieren zieht weitere Rechtsfolgen nach sich. Einer Forderung sollte, gegebenenfalls mit anwaltlicher Unterstützung, fristgerecht entgegengetreten werden; Nutzerdaten sollten keinesfalls voreilig weitergegeben werden.

## 8. Anhang

Quelle für Gesetzestexte im Internet: [www.gesetze-im-internet.de](http://www.gesetze-im-internet.de)  
(*Informationsangebot des Bundesministeriums der Justiz*)

Im Text erwähnte Urteile:

### **Bundesgerichtshof**

BGH-Urteil vom 15.11.2012, I ZR 74/12  
BGH-Urteil vom 13.01.2011, III ZR 146/10  
BGH-Urteil vom 12.07.2007, I ZR 18/04

### **Bundesverfassungsgericht**

BVerfG-Urteil vom 02.03.2010, 1 BvR 256/08



VAF Bundesverband Telekommunikation e.V.  
Otto-Hahn-Str. 16, 40721 Hilden  
[www.vaf-ev.de](http://www.vaf-ev.de)