



# Das Unternehmen als Internet Access Provider

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



*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 unter besonderer Berücksichtigung von WLAN

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

### Verfasser des Gutachtens

Rechtsanwalt Wolfgang Müller, Fachanwalt für Informationstechnologierecht, Kanzlei Schlüter Graf Rechtsanwälte PartG mbB in Dortmund; Lehrbeauftragter der Technischen Universität Dortmund an der Fakultät für Informatik sowie Lehrbeauftragter der Fachhochschule Dortmund im Fachbereich Informatik

### Hinweis zur 3. Auflage 2016

Das Gutachten und diese Zusammenfassung wurden vom Verfasser erneut darauf hin überprüft, ob aufgrund neuer Rechtsprechung und Gesetzgebung die in der ersten Auflage getroffenen Aussagen korrigiert werden müssen. Nach erfolgter Prüfung wird auch in der aktualisierten Version des Gutachtens die Auffassung vertreten, dass die bereits in der Ursprungsfassung des Gutachtens vertretenen Ergebnisse unverändert Anwendung finden. Die Berücksichtigung der jüngeren Rechtsentwicklung in der Darstellung hat somit lediglich eine erläuternde Funktion.

### Hinweis zur 2. Auflage 2013

Das Gutachten und diese Zusammenfassung wurden im Sommer 2013 vom Verfasser darauf hin überprüft, ob aufgrund neuer Rechtsprechung und Gesetzgebung die in der ersten Auflage getroffenen Aussagen korrigiert werden müssen. Nach erfolgter Prüfung wird die Auffassung vertreten, dass die bereits 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 mitberücksichtigt, das auch in seiner Begründung der hier bereits vertretenen Auffassung entspricht.

### Hinweis zur 1. Auflage 2011

Das vorliegende Dokument fasst wesentliche Ergebnisse eines Rechtsgutachtens zusammen, das vom Verfasser Rechtsanwalt Wolfgang Müller im Auftrag des VAF Bundesverband Telekommunikation e. V. erarbeitet und im Juli 2011 fertiggestellt wurde.

### Herausgeber

VAF Bundesverband Telekommunikation e. V.

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

1. Vorsitzender: Hans A. Becker; Geschäftsführer: Martin Bürstenbinder

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

**Redaktion:** Martin Bürstenbinder, VAF e. V.; Redaktionsassistentz: Julia Noglik, VAF e. V.

**Layout:** Uwe Klenner, [www.layout-und-gestaltung.de](http://www.layout-und-gestaltung.de); **Lektorat:** ad litteras

**Copyright:** VAF e. V. Oktober 2016. Dritte, aktualisierte 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 auf dem Erkenntnisstand zum Zeitpunkt der Fertigstellung basiert. 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. Warum eine aktualisierte, dritte Fassung 2016?
2. Einleitung
3. Begriffe
4. Keine Haftung für fremde Informationen
5. Sicherheit ja, Überwachung nein
6. Enge Grenzen für Speicherung und Weitergabe von Daten
  - 6.1 Datenschutz und Fernmeldegeheimnis
  - 6.2 Vorratsdatenspeicherung
  - 6.3 Daten für Abrechnungs- und für technische Zwecke
7. Kommentar
8. Praxishinweise
9. Anhang

## 1. Warum eine aktualisierte, dritte Fassung 2016?

Im Sommer 2016 bin ich vom VAF Bundesverband Telekommunikation e. V. erneut gebeten worden, das von mir im Jahr 2011 in seiner ersten Fassung erstellte Rechtsgutachten nun wieder, wie bereits im Jahr 2013, einer kritischen Revision zu unterziehen. Es war also zu prüfen, ob sich die seitherigen Entwicklungen und gerade auch die in der Öffentlichkeit jüngst mit großer Anteilnahme verfolgten Geschehnisse auf die zuvor getroffenen Aussagen auswirken.

Im Rampenlicht der Kommentierungen stand die als großer Sprung nach vorn angekündigte Änderung des Telemediengesetzes (TMG), die am 21.07.2016 dann in nur stark reduzierter Form erfolgte – und sich letztlich als bescheidener Tritt auf der Stelle manifestierte. Von dem ursprünglichen Entwurf verblieb im Wesentlichen lediglich ein einzelner Satz, der als neu eingefügter Absatz 3 im § 8 TMG die in der hier zugrunde liegenden Untersuchung bereits wiederholt vertretene Auffassung bekräftigt. Wer Kunden, Gästen usw. über ein WLAN-Netz den Internetzugang ermöglicht, ist den sonstigen Internetzugangsanbietern in der Hinsicht gleichgestellt. Somit gilt weiterhin, dass der Netzzugangsanbieter nicht unmittelbar für Schadenersatzansprüche aus Urheberrechtsverletzungen haftet, die ein Dritter ohne Veranlassung des WLAN-Netzbetreibers über das WLAN als Internetzugang verursacht hat. Gleichwohl setzt sich der Betreiber des WLAN-Netzes auch künftig dem Risiko der sogenannten Störerhaftung – somit der damit verbundenen Abmahn- und Gerichtskosten – aus, sofern er für den Betrieb seines WLAN-Netzes keine dafür gebotenen Sicherungsmaßnahmen vorsieht, die auf die Beseitigung oder Unterlassung von darüber erfolgten Rechtsverletzungen zielen.

Diese Auffassung bringt auch der Europäische Gerichtshof (EuGH) in seinem Urteil vom 15.09.2016 zum Ausdruck. Ob allerdings die vom EuGH geforderte Möglichkeit, im Bedarfsfall die Identität des mutmaßlichen Rechtsverletzers aufdecken zu können, durch ein Verfahren der Passwortvergabe mit Bekanntgabe der Identität tatsächlich greifen kann, muss für die praktische Anwendung vielfach als fraglich gelten. So dürfte allein aufgrund der Registrierung im Streitfall oftmals wohl kaum feststellbar sein, von welchem registrierten Nutzer der durch ein Passwort geschützte WLAN-Zugang zu einer Urheberrechtsverletzung missbraucht worden ist.

Was bleibt ist, dass jedermann sich an das geltende Recht zu halten hat. Gut beraten war und ist darum als Betreiber, wer – insbesondere auch unter Beachtung der datenschutzrechtlichen Vorgaben – konsequent sein WLAN-Netz sichert und dessen Nutzung durch Gäste oder Kunden mit einer Form der Zugangskontrolle verknüpft.

Inhaltlich und somit auch in den Ergebnissen bleiben die wesentlichen Aussagen des Gutachtens unverändert zu denen der beiden ersten Fassungen.

*Dortmund, 5. Oktober 2016      Wolfgang Müller,  
Fachanwalt für Informationstechnologierecht*

## 2. Einleitung

Soweit Unternehmen generell oder an speziellen Orten wie z. B. die Deutsche Bahn in Bahnhöfen oder in Zügen, die Betreiber von Flughäfen in der Wartehalle, 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.

Eine heute weitverbreitete Bereitstellungsform des Internetzugangs für Gäste ist das Angebot eines WLAN.

Wiederholt werden 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 in seiner jüngsten Revisionsfassung wiederum als wesentliches Ergebnis die Klarstellung, dass das bloße Angebot des Zugangs zum Internet keine Haftung des gewerblichen Zugangsanbieters für eventuelle Rechtsverletzungen durch Nutzer verursacht. Gleichwohl gilt auch weiterhin, dass dem Angebot »offener WLAN-Hotspots«, d. h. solcher WLANs ohne Sicherung und Zugangskontrolle, eine Absage erteilt wird.

Die für Betreiber von Hotels, Cafés, Krankenhäusern usw. wesentlichen Ergebnisse der rechtlichen Begutachtung werden in der hier vorliegenden Zusammenfassung dargestellt und dabei die maßgeblichen Rechte und Pflichten erläutert, die für das gesetzeskonforme Angebot von Internetzugängen durch ein Unternehmen zu beachten sind.

### 3. 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](http://spiegel.de) oder [t-online.de](http://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)*

### 4. 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 (»Schadenersatz«) 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.

(3) Die Absätze 1 und 2 gelten auch für Diensteanbieter nach Absatz 1, die Nutzern einen Internetzugang über ein drahtloses lokales Netzwerk zur Verfügung stellen.

**Hinweis:** Der Absatz 3 wurde am 21.07.2016 neu und als Ergänzung in den § 8 TMG aufgenommen. Dadurch bekräftigt der Gesetzgeber (lediglich), dass die Bestimmungen des § 8 TMG gleichermaßen auch für Betreiber eines »drahtlosen lokalen Netzwerks«, d. h. eines WLAN, gelten.

## 5. 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 Verfahrens der Verschlüsselung sowie der individuellen Zuteilung von Nutzungsberechtigungen.

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 [BGH] vom 12.07.2007).

Ebenso ist zu beachten, dass dem Access Provider 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.

Beispiel 1: Zwar lehnt der BGH in seinem Urteil vom 08.01.2014 die Kontroll- und vorbeugende Belehrungspflicht des Anschlussinhabers gegenüber einem im Haushalt lebenden, volljährigen Stiefsohn ab. Jedoch wird auch ausgeführt, dass sich dies anders darstellen könne, wenn bereits konkrete Anhaltspunkte für eine rechtswidrige Nutzung durch ein volljähriges Haushalts- bzw. Familienmitglied vorliegen. Beispiel 2: Zwar lehnt der BGH in seinem Urteil vom 15.11.2012 das grundsätzliche Vorliegen einer ständigen Pflicht zur Kontrolle der Internetnutzung von Minderjährigen durch die Erziehungsberechtigten ab. Allerdings muss es als durchaus zumutbar gelten, dass Minderjährige von Eltern eingewiesen und stichprobenartig beaufsichtigt werden.

Umso offensichtlicher ist vor dem Hintergrund der beiden Beispiele, dass diese häuslichen Verhältnisse nicht auf eine gewerbliche Situation, wie in einem Hotel, Café, Krankenhaus oder der Wartehalle eines Flughafens, übertragen werden können. Dementsprechend ist auch die verschiedentlich vorgebrachte Auffassung irrtümlich, dass ein gewerblicher Access Provider Gäste vor der Nutzung seines WLANs z.B. durch AGB über rechtmäßiges Verhalten im Internet belehren müsse.

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

### 6.1 Datenschutz und Fernmeldegeheimnis

**Die Bestimmungen zum Datenschutz und zum 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 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.

## 6.2 Vorratsdatenspeicherung

**Ein gesetzlicher Ausnahmetatbestand, der die ausnahmsweise Speicherung von Nutzungs-/Verkehrsdaten auf Vorrat zulässt, ist derzeit nicht gegeben. Zwar hat der deutsche Gesetzgeber bestimmt, dass ab dem 01.07.2017 diesbezüglich neue Vorgaben umzusetzen sind. Jedoch hat das Bundesverfassungsgericht in der dazu anhängigen Klage noch nicht geurteilt.**

Bereits die vormaligen §§ 113a (Speicherungspflichten für Daten) und 113b (Verwendung der nach § 113a gespeicherten Daten) TKG waren 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 02.03.2010 unverzüglich zu löschen gewesen.

Zwar hat der deutsche Gesetzgeber am 10.12.2015 mit dem »Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten« eine Neuregelung der Speicherungspflichten in den §§ 113a bis 113f TKG vorgenommen und die Diensteanbieter verpflichtet, diese ab dem 01.07.2017 umzusetzen. Allerdings wurde auch gegen diese neuerliche Regelung Klage beim Bundesverfassungsgericht erhoben. Zu der Frage, ob und gegebenenfalls welche neuen Vorgaben für die Speicher- und Löschpflichten von Access Providern ab dem 01.07.2017 gelten werden, kann somit gegenwärtig und vor Verkündung eines Urteils des Bundesverfassungsgerichts keine verlässliche Aussage getroffen werden.

## 6.3 Daten für Abrechnungs- und für technische Zwecke

Für die Speicherung und Löschung von Nutzungs-/Verkehrsdaten gilt zum Zeitpunkt dieser Veröffentlichung:

**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 dem Urteil des BGH vom 13.01.2011 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.

## 7. Kommentar

Immer wieder halten Diskussionen rund um (vermeintliche) gesetzliche Neuerungen im Bereich des Betriebs von gerade auch gewerblichen WLAN-Netzen mit Gastzugängen die Öffentlichkeit und insbesondere die Betreiber selbst – die Access Provider – in Atem. Gleichwohl hat sich seit der Erstauflage dieses Gutachtens im Jahr 2011 keine grundlegend neue Situation ergeben. Schlussendlich besteht die gesellschaftliche Herausforderung darin, die berechtigten Belange aller Verkehrskreise in einer verfassungskonformen Gesetzesreform in Einklang zu bringen. Ob und wann die politische Willensbildung in Deutschland und Europa dafür reif sein wird, kann und soll hier nicht beurteilt werden. Weiterhin gilt jedoch: Vom Access Provider kann nicht mehr verlangt werden, als sich gesetzestreu zu verhalten.

## 8. Praxishinweise

- Unternehmen wie Hotels, Krankenhäuser usw. dürfen ihren Gästen, Patienten usw. Internetzugänge anbieten. Sie sind dann Internet Access Provider. Eine häufig verwendete Bereitstellungsform ist der Internetzugang mittels eines WLAN.
- 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.

## 9. Anhang

Quelle für Gesetzestexte im Internet:

**[www.gesetze-im-internet.de](http://www.gesetze-im-internet.de)**

*(Informationsangebot des Bundesministeriums der Justiz)*

Höchstrichterliche Urteile:

### **Bundesgerichtshof**

BGH-Urteil vom 08.01.2014, I ZR 169/14;  
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

### **Europäischer Gerichtshof**

EuGH-Urteil vom 15.09.2016, C-484/14



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