Rechtliche Anforderungen an öffentliches WLAN
Informationsblatt für WLAN-Betreiber

Immer wieder sind rechtliche Anforderungen an öffentliches WLAN Thema in den Medien. Grundsätzlich gilt, dass die aktuelle Rechtslage immer nur eine Momentaufnahme ist, die sich binnen weniger Monate durch Anpassungen von Gesetzen oder sogar plötzlich durch klarstellende Gerichtsurteile ändern kann.

Den Überblick über die jeweils gültige Gesetzeslage zu behalten, Änderungen zu verfolgen und die daraus resultierenden neuen Anforderungen umzusetzen, ist ein Teil der Leistungen, die HOTSPLOTS seinen Kunden im Rahmen seines WLAN-Service erbringt.

Wir informieren Sie in diesem Informationsblatt über:

Erfüllung aller rechtlichen Anforderungen

Eine professionelle Hotspot-Lösung, wie sie von HOTSPLOTS angeboten wird, bietet Rechtssicherheit.

Der rechtskonforme Betrieb eines WLAN-Hotspots erfordert die Einhaltung einer Vielzahl von Vorschriften aus geltenden Gesetzen und Verordnungen, wie etwa dem Telekommunikationsgesetz (TKG), dem Telemediengesetz (TMG), dem Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG), der EU-Datenschutzgrundverordnung (DSGVO), dem Verbraucher- und Jugendschutz und ggf. der Telekommunikationsüberwachungsverordnung (TKÜV).

Die Betreiber der öffentlichen Netze sind gegebenenfalls auskunftspflichtig gegenüber Behörden. § 22 ff. TTDSG sieht ein „Auskunftsverfahren“ vor. Hier greift durch HOTSPLOTS der Schutz des Standortinhabers auch bei schweren Straftaten (Terrorismus etc.), die mit Themen wie der Störerhaftung oder Netzsperren gar nichts zu tun haben. Es gilt zwar das Täter-Prinzip, aber schon die Anfragen der Ermittlungsbehörden (z. B. durch das BKA) kosten Unternehmen Zeit und sollten schnell und professionell bearbeitet werden. In besonders schweren Fällen können den Unternehmen sogar Hausdurchsuchungen drohen. Bei HOTSPLOTS werden die Anfragen qualifiziert, effektiv und diskret bearbeitet – in direktem Austausch mit den Behörden.

Bei Bedarf involviert HOTSPLOTS externe Juristen der jeweiligen Fachbereiche, sowie den für HOTSPLOTS zuständigen externen Datenschutzbeauftragten zur Lösung der jeweiligen Themenkomplexe. Insbesondere bei der Lösungsfindung in Datenschutzangelegenheiten erfolgt, sofern nötig, eine enge Abstimmung zwischen dem Kunden, HOTSPLOTS und dem externen Datenschutzbeauftragten.

hotsplots GmbH, Rotherstr. 22, 10245 Berlin – Website: www.hotsplots.de – E-Mail: info@hotsplots.de
Geschäftsführer: Dipl.-Ing. Sascha Schaub– USt-IdNr.: DE237345081 – Register: Amtsgericht Charlottenburg HRB 93460B

HOTSPLOTS ist seit 2004 bei der Bundesnetzagentur als WLAN-Access-Provider registriert und stellt das Sicherheitskonzept für die Einhaltung geforderter Auflagen regelmäßig bereit.

Mit HOTSPLOTS können sich die Kunden auf ihr eigenes Geschäft konzentrieren. Ändert sich die Rechtslage, so setzt HOTSPLOTS die Änderungen zentral um. Zudem schützt das VPN-Routing die Identität des Standortinhabers bei Missbrauch der Internetverbindung jeglicher Art und bietet somit einen Schutz vor Rechtsfolgen.

TMG - Statt Störerhaftung Netzsperren eingeführt

Mit dem „Dritten Gesetz zur Änderung des Telemediengesetzes“ vom 13. Oktober 2017 wurden einklagbare „Netzsperren“ eingeführt. Ein Urteil des Bundesgerichtshofs hat die Abschaffung der Störerhaftung zwar im Juli 2018 bestätigt, aber die Unsicherheit über die Netzsperren noch vergrößert, indem es in einer Mitteilung zum Urteil den Begriff der Sperrung sehr weit auslegt: „Der Anspruch auf Sperrmaßnahmen ist nicht auf bestimmte Sperrmaßnahmen beschränkt und kann auch die Pflicht zur Registrierung von Nutzern, zur Verschlüsselung des Zugangs mit einem Passwort oder – im äußersten Fall – zur vollständigen Sperrung des Zugangs umfassen“ [1]. Auch diese Unsicherheit ist ein Grund, warum man als Anbieter eines öffentlichen WLAN auf einen professionellen Provider wie HOTSPLOTS setzen sollte, der neue rechtliche Anforderungen, wie zum Beispiel Sperrmaßnahmen, umsetzen kann.

Konkret heißt es in § 7 des Telemediengesetzes (TMG) in der aktuellen Fassung vom 12. August 2021 in den Abschnitten 3 und 4[2]:

> *„(3) Verpflichtungen zur Entfernung von Informationen oder zur Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen aufgrund von gerichtlichen oder behördlichen Anordnungen bleiben auch im Falle der Nichtverantwortlichkeit des Diensteanbieters nach den §§ 8 bis 10 unberührt. Das Fernmeldegeheimnis nach § 3 des Telekommunikation-Telemedien-Datenschutz-Gesetzes ist zu wahren.*
>
> *(4) Wurde ein Telemediendienst von einem Nutzer in Anspruch genommen, um das Recht am geistigen Eigentum eines anderen zu verletzen und besteht für den Inhaber dieses Rechts keine andere Möglichkeit, der Verletzung seines Rechts abzuhelfen, so kann der Inhaber des Rechts von dem betroffenen Diensteanbieter nach § 8 Absatz 3 die Sperrung der Nutzung von Informationen verlangen, um die Wiederholung der Rechtsverletzung zu verhindern. Die Sperrung muss zumutbar und verhältnismäßig sein. Ein Anspruch gegen den Diensteanbieter auf Erstattung der vor- und außergerichtlichen Kosten für die Geltendmachung und Durchsetzung des Anspruchs nach Satz 1 besteht außer in den Fällen des § 8 Absatz 1 Satz 3 nicht.“*

TKG - Meldepflicht

Das Telekommunikationsgesetz (TKG) sieht unter § 5[3] eine Meldepflicht für *„gewerblich öffentliche Telekommunikationsnetze“* und „gewerblich öffentlich zugängliche Telekommunikationsdienste“ vor.

Ausgenommen von der Meldepflicht sind „beispielsweise Betreiber von (Internet)Cafés, Einkaufszentren, Hotels/Restaurants mit WLAN-Angebot, Hotspots“, da das „Ermöglichen [einer] kurzzeitigen (Mit-)Nutzung eines Internetzugangsdienstes […] nicht als „Erbringen eines Telekommunikationsdienstes“ i. S. d. § 5 Absatz 1 Satz 1, 2. Alt. TKG angesehen“ wird (Veröffentlichung im Amtsblatt 23-2021 vom 8.12.2021)[4]. Betreiber öffentlicher

1 http://www.heise.de/newsticker/meldung/Analyse-Stoererhaftung-durch-neue-Rechtsunsicherheiten-ersetzt-4121377.html
2 https://www.gesetze-im-internet.de/tmg/BJNR017910007.html
3 https://dejure.org/gesetze/TKG/5.html
4 Mitteilung Nr. 324/2021 abrufbar unter https://www.bnetza-amtsblatt.de/download/73

Telekommunikationsnetze sowie gewerbliche Anbieter von Telekommunikationsanschlüssen zur selbstständigen Verwendung sind weiterhin meldepflichtig.

Für meldepflichtige Betreiber bzw. Anbieter besteht die Anforderung, neben der Anmeldung bei der Bundesnetzagentur, ein Sicherheitskonzept einzureichen. So heißt es in § 166 TKG Zi. 2[5]:

„(1) Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat

1. einen Sicherheitsbeauftragten zu bestimmen,

2. einen in der Europäischen Union ansässigen Ansprechpartner zu benennen und

3. ein Sicherheitskonzept zu erstellen ,[…]

(2) Wer ein öffentliches Telekommunikationsnetz betreibt, hat der Bundesnetzagentur das Sicherheitskonzept unverzüglich nach der Aufnahme des Netzbetriebs vorzulegen. Wer öffentlich zugängliche Telekommunikationsdienste erbringt, kann von der Bundesnetzagentur verpflichtet werden, das Sicherheitskonzept vorzulegen. […]

(3) Mit dem Sicherheitskonzept ist eine Erklärung vorzulegen, dass die in dem Sicherheitskonzept aufgezeigten technischen Vorkehrungen und sonstigen Schutzmaßnahmen umgesetzt sind oder unverzüglich umgesetzt werden.

(4) Stellt die Bundesnetzagentur im Sicherheitskonzept oder bei dessen Umsetzung Sicherheitsmängel fest, so kann sie die unverzügliche Beseitigung dieser Mängel verlangen. Sofern sich die dem Sicherheitskonzept zugrunde liegenden Gegebenheiten ändern, hat der nach Absatz 2 Verpflichtete das Sicherheitskonzept unverzüglich nach der Änderung anzupassen und der Bundesnetzagentur unverzüglich nach erfolgter Anpassung unter Hinweis auf die Änderungen erneut vorzulegen.

(5) Die Bundesnetzagentur überprüft regelmäßig die Umsetzung des Sicherheitskonzepts. Die Überprüfung soll mindestens alle zwei Jahre erfolgen.“

Mit HOTSPLOTS Bereitstellungsverträgen besteht garantiert keine Meldepflicht für Sie als Kunde und Ihr Standort wird in das Sicherheitskonzept von HOTSPLOTS aufgenommen.

Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (Vorratsdatenspeicherung)

Im Mai 2015 hat das Bundesministerium der Justiz und Verbraucherschutz das „Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“[6] vorgelegt. Im Oktober 2015 wurde es beschlossen und ist am 18.12.2015 in Kraft getreten. Für Unternehmen wurde die Frist zur Umsetzung bis zum 01.07.2017 festgelegt.

Am 28.06.2017 wurde diese Speicherverpflichtung nach § 176 TKG (§ 113b a. F.) von der Bundesnetzagentur ausgesetzt[7] - nicht abgeschafft.

Es bleibt abzuwarten, wie die Gerichte über die anhängigen Eilanträge entscheiden werden. Die aktuelle Rechtsprechung z. B. vom Verwaltungsgericht Köln („Keine Pflicht für Telekommunikationsunternehmen zur Vorratsdatenspeicherung“)[8] lässt ein Berufungsverfahren oder eine Sprungrevision zum Bundesverwaltungsgericht

5 https://dejure.org/gesetze/TKG/166.html
6 https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/BGBl_Hoechstspeicherfrist.pdf
7 https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/OeffentlicheSicherheit/Ueberwachung_Auskunftsert/VDS_113aTKG/node.html
8 http://www.vg-koeln.nrw.de/behoerde/presse/Pressemitteilungen/01_180420/index.php

zu. Die aktuelle Rechtsprechung bezieht sich noch auf altes EU-Recht (Richtlinie 2002/58). Mit dem 25.5.2018 ist die neue EU-Verordnung (COM(2017)10 final) in Kraft getreten.

In der EU-Verordnung (COM(2017)10 final) steht dazu folgender Absatz[9]:

> *„Der vorliegende Vorschlag enthält keine besonderen Bestimmungen in Bezug auf die Vorratsdatenspeicherung. Er behält den wesentlichen Inhalt des Artikels 15 der e-Datenschutz-Richtlinie bei und passt ihn an den besonderen Wortlaut des Artikel 23 der DS-GVO an, der Gründe vorsieht, aus denen die Mitgliedstaaten den Umfang der aus bestimmten Artikeln der e-Datenschutz-Richtlinie erwachsenden Rechte und Pflichten einschränken können.* ***Daher steht es den Mitgliedstaaten frei, nationale Rahmen für die Vorratsdatenspeicherung zu schaffen oder beizubehalten, die u. a. gezielte Vorratsspeicherungen vorsehen, sofern solche Rahmen unter Beachtung der Rechtsprechung des Gerichtshofs der Europäischen Union zur Auslegung der e-Datenschutz-Richtlinie und der Charta der Grundrechte mit dem Unionsrecht vereinbar sind.*** *“*

Auch eine Entscheidung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung ist offen[10]. Je nachdem wie diese Entscheidung ausfällt, wäre die Bundesnetzagentur wieder verpflichtet, das Gesetz durchzusetzen. Grundsätzlich gilt: Sollte die Vorratsdatenspeicherung zur Verpflichtung werden, ist sie für alle Telekommunikationsdienstleiter verpflichtend, egal, welche Größe, oder welche Nutzerzahlen das Unternehmen hat.

Die aktuelle Vorratsdatenspeicherung von 2017 ist mit weit reichenden technischen Auflagen verbunden, die ein WLAN-Betreiber nicht ohne erheblichen Aufwand erfüllen kann – hinzu kommt, dass empfindliche Geldstrafen bei Verstößen angedroht und vollstreckt werden können. Zu den Anforderungen einer Umsetzung zählen voraussichtlich:

- Vier-Augen-Prinzip und Speicherung von Daten auf Systemen, die nicht mit dem Internet verbunden sind.
- Ein Audit und erhöhte Sicherheitsanforderungen wie Verschlüsselung und Protokollierung.

Datenschutzgrundverordnung (DSGVO)

Seit Mai 2018 gilt die EU-weite, einheitliche Datenschutzverordnung. Personenbezogene Daten u. a. auch Verkehrsdaten wie MAC-Adressen, Session-IDs, Nutzungsdauer oder Datenmengen, die eventuell von der eingesetzten Hardware (Hotspot-Router) gespeichert oder übertragen werden, unterliegen den Regelungen der DSGVO.

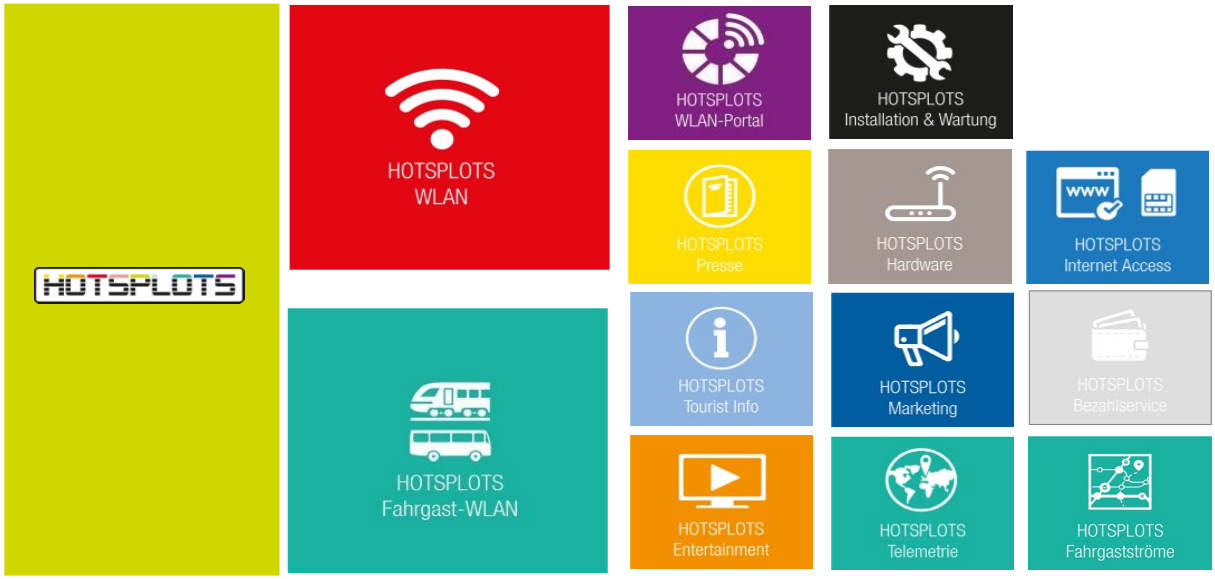
Kundenanfragen zu personenbezogenen Daten, Anfragen zur Datenlöschung und Speicher- und Löschfristen sind von einem WLAN-Betreiber nach der DSGVO zu dokumentieren und unverzüglich zu bearbeiten.

HOTSPLOTS involviert bei Bedarf den für HOTSPLOTS zuständigen externen Datenschutzbeauftragten zur Lösung der jeweiligen Themenkomplexe. Insbesondere bei der Lösungsfindung in Datenschutzangelegenheiten erfolgt, sofern nötig, eine enge Abstimmung zwischen dem Kunden, HOTSPLOTS und dem externen Datenschutzbeauftragten.

9 https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:52017PC0010, Abschnitt: „1.3., Absatz 3
10 https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/06/rk20160608_1bvr022916.html, Abschnitt 27

Vielfältige Mehrwerte für Hotspot-Betreiber – alles aus einer Hand

HOTSPLOTS ist mehr als nur rechtskonformes Gäste-WLAN und bietet äußerst skalierbare Hotspot-Lösungen, die entsprechend dem jeweiligen Bedarf mit unterschiedlichen Mehrwerten erweitert werden können. Die Funktionalitäten von HOTSPLOTS Marketing ermöglichen eine Interaktion mit dem Nutzer und machen das Gäste-WLAN zum Kommunikationskanal. Die Lösungen von HOTSPLOTS Presse und Entertainment erweitern diese Vorteile zusätzlich mit Zeitungen und Zeitschriften oder Video-Inhalten.



Alle Informationen sind zu finden unter https://hotsplots.com/produkte/

Haben Sie weitere Fragen zu uns und unseren Produkten? Dann rufen Sie uns einfach an (+49 30 29 77 348-84).

Vertrieb, hotsplots GmbH

Berlin, Dezember 2022