Häufig gestellte Fragen zur Rechtslage bei gewerblichen öffentlichen WLAN Angeboten in Deutschland

1. Allgemein

Welche Gesetze und Verordnungen müssen beachtet werden?

Es gilt das Telekommunikationsgesetz (TKG) vom 22.06.2004, wobei die Erleichterungen gemäß § 150 Abs. 12 lit. b TKG seit 01.01.2009 nicht mehr gelten. Daneben gilt grundsätzlich auch die Telekommunikations-Überwachungsverordnung (TKÜV) vom 22.01.2002, zuletzt geändert durch Gesetz vom 25.12.2008. Darüber hinaus greift das Telemediengesetz (TMG) vom 26.02.2007 regelnd ein, zuletzt geändert durch Artikel 1 des Gesetzes vom 31.05.2010. Weiter gelten das Bundesdatenschutzgesetz (BDSG) vom 20.12.1990 in der Neufassung vom 14.01.2003, zuletzt geändert durch Gesetz vom 14.08.2009, und die jeweiligen Datenschutzgesetze der Länder. Daneben ist insbesondere auf die Einhaltung des Urheberrechtsgesetzes (UrhG) und der übrigen Gesetze, insbesondere des UWG etc., zu achten.

Welche Gerichtsurteile sollten beachtet werden?

Zu beachten ist die Rechtsprechung zu einer möglichen Störerhaftung bei (ungesichertem) WLAN-Funknetz im Falle von Urheberrechtsverletzungen, hier haben insbesondere die Landgerichte Hamburg, Frankfurt und Mannheim eine Haftung des WLAN-Betreibers angenommen. Mit weiteren (verwaltungsgerichtlichen) Urteilen in der Umsetzung der jetzt erweitert geltenden Bußgeldvorschriften gemäß § 149 TKG ist zu rechnen.

Muss ein Hotspot angemeldet werden?

Nach der herrschenden Meinung werden auch offene WLAN-Netze von der Meldepflicht des § 6 TKG grundsätzlich erfasst, wonach der gewerbliche Anbieter von Telekommunikationsdiensten für die Öffentlichkeit meldepflichtig ist. Die Frage der Gewerblichkeit ist im Einzelfall zu prüfen.

2. Nutzerdatenerfassung , -speicherung und Schutz

Müssen Daten der Nutzer (Endkunden) gespeichert werden?

Die herrschende Meinung geht davon aus, dass die Vergabe dynamischer IP-Adressen unter TKG §111 fällt, sodass Bestandsdaten gespeichert werden müssen.

Das Bundesverfassungsgericht hat in seinem Urteil vom 02.03.2010 für Recht erkannt, dass die §§ 113 a und 113 b des Telekommunikationsgesetzes (TKG) sowie § 100 g Abs. 1 Satz 1 der Strafprozessordnung (StPO) gegen Artikel 10 des Grundgesetzes verstoßen und damit nichtig sind. Damit ist die Verpflichtung zur Speicherung von Verkehrsdaten auf Vorrat unter anderem zum Zweck der Verfolgung von Straftaten ab sofort weggefallen.

Darüber hinaus dürfen Dienste-Anbieter gemäß § 96 ff TKG teilweise Verkehrsdaten weiterhin für die dort genannten Zwecke u.a. zur Entgeltabrechnung erheben und verwenden.

Was versteht man unter Bestandsdaten, was unter Verkehrsdaten?

Unter Bestandsdaten versteht das Gesetz in diesem Fall die IP-Adresse, Name und Anschrift des „Anschlussinhabers" sowie dessen Geburtsdatum.

Die Speicherung von Verkehrsdaten umfasst die dem Teilnehmer für die Internetnutzung zugewiesene IP-Adresse, eine eindeutige Anschlusskennung, über den die Internet-Nutzung erfolgte, sowie Beginn und Ende der Internet-Nutzung nach Datum und Uhrzeit unter Angabe der zu Grunde liegenden Zeitzone.

Reicht eine E-Mail Adresse zum Nutzungsnachweis?

Eine E-Mail-Adresse reicht nach herrschender Meinung nicht aus, bezüglich der Bestandsdaten einen ausreichenden Nachweis zu führen, da ohne Weiteres E-Mailadressen anonym erworben werden können.

Ist die Verpflichtung zur Vorratsdatenspeicherung von Verkehrsdaten mit dem BVerfG-Urteil dauerhaft vom Tisch?

Das Bundesverfassungsgericht hat ausdrücklich klargestellt, dass das Grundgesetz eine Speicherung von Verkehrsdaten auf Vorrat „nicht unter allen Umständen verbietet". Soweit sich die Umsetzung der EU-Richtlinie 2006/24/EG in nationales Recht genau an die Vorschriften dieser Richtlinie halte, könne die Richtlinie auch ohne Verstoß gegen das Grundgesetz wirksam umgesetzt werden.

Mit dieser klaren Rechtsmeinung öffnet das Bundesverfassungsgericht dem Gesetzgeber die Tür für ein neues, dieses Mal verfassungsgemäßes „Gesetz zur Vorratsdatenspeicherung", mit einer Umsetzung durch den Gesetzgeber ist zu rechnen.

Inwieweit müssen die Daten von The Cloud auf Glaubwürdigkeit geprüft werden?

Die Vorschriften des TKG, insbesondere § 95 Abs. 4 TKG, verlangen vom Diensteanbieter nicht, dass er die Angaben des Endkunden und Nutzers überprüft. Der Diensteanbieter darf sich einen amtlichen Ausweis vorlegen lassen, er ist jedoch nicht jedoch dazu verpflichtet.

Wie werden die Daten von The Cloud erfasst?

Je nach Servicevariante wendet The Cloud unterschiedliche Verfahren zur Erfassung der Daten und Identifizierung der Nutzer an:

Bei Endkundennutzung über Roamingpartner und bei Mobilfunk– und Kreditkartenzahlern wird eine Rückverfolgung über entsprechende Vereinbarungen mit den Dienstleistern gewährleistet. Bei temporären Buchungen von Zugängen vor Ort stellt The Cloud ein elektronisches Buchungssystem zur Verfügung, das die Erfassung der Endkundendaten durch das Personal vor Ort ermöglicht.

In allen Varianten wird die dem Endkunden zugewiesene IP-Adresse dem Datensatz automatisch zugefügt, sodass eine Nachverfolgung der Nutzung möglich wird.

Bei Verkauf von Vouchern müssen die Mitarbeiter der Einrichtung (Hotel etc.) die Bestandsdaten erfassen (The Cloud Formular zur Bestandsdaten-Erfassung) - also Name, Adresse, Geburtsdatum und Abgabezeitpunkt- und diese mit Ablauf des auf die Vertragsbeendigung folgenden Kalenderjahres löschen.

Wie erfolgt die Zuordnung der Nutzerdaten zur IP-Adresse der getätigten Verbindung?

Die Nutzungsdaten inkl. IP Adresse, Identifikationsadresse der Hardware (Notebook bzw. WLAN-Karte) werden zu Beginn und Ende jeder Nutzung in Datenbanken gespeichert.

Wie lange müssen oder dürfen diese Daten gespeichert werden?

Bestandsdaten sind zunächst unbefristet zu speichern und erst mit Ablauf des auf die Beendigung des Vertragsverhältnisses folgenden Kalenderjahres zu löschen.

§ 97 Abs. 3 TKG bestimmt, dass die für die Berechnung des Entgelts erforderlichen Verkehrsdaten bis zu sechs Monate nach Versendung der Rechnung gespeichert werden dürfen. Für die Abrechnung nicht erforderliche Daten sind unverzüglich zu löschen. Jede unzulässige Erhebung und Verwendung von Verkehrsdaten ist gleichzeitig ein Verstoß gegen das Bundesdatenschutzgesetz und wird nach dem TKG mit Strafe bedroht.

Wem müssen/dürfen diese Daten herausgegeben werden?

Rechtsgrundlage für die Eingriffe in das Fernmeldegeheimnis, nämlich die Herausgabe gespeicherter Daten, sind insbesondere die Strafprozessordnung und das Gesetz zu Art. 10 Grundgesetz. Das TKG regelt nur die Vorgaben für die technische Umsetzung solcher Überwachungsmaßnahmen und für die Erteilung von Auskünften. Auskünfte aus den Bestandsdaten sind demnach den Gerichten und Strafverfolgungsbehörden, den Polizeivollzugsbehörden des Bundes und der Länder, dem Zollkriminalamt und den Zollfahndungsämtern, den Verfassungsschutzbehörden des Bundes und der Länder, dem militärischen Abschirmdienst und dem Bundesnachrichtendienst sowie weiteren Behörden zur Verfügung zu stellen.

Welche Datenschutzbestimmungen sind zu beachten?

Es sind die Bestimmungen des Bundesdatenschutzgesetzes sowie der Datenschutzgesetze der Länder zu beachten sowie insbesondere die Regelungen der §§ 91 ff. TKG: Danach sind die Nutzer vom Diensteanbieter über Erhebung und Verwendung personenbezogener Daten zu unterrichten. Bestandsdaten dürfen dabei für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung des Vertragsverhältnisses erhoben werden, wenn dies erforderlich ist bzw. zur Erfüllung der vorgenannten Rechtspflichten. Verkehrsdaten dürfen erhoben werden, soweit dies zum Aufbau bzw. zur Aufrechterhaltung der Telekommunikation erforderlich ist sowie ebenfalls zur Erfüllung der Informationspflichten gegenüber den Strafverfolgungsbehörden.

3. Haftungsrisiken

Welches Risiko besteht im Falle der Missachtung dieser Rechtsvorschriften für den Betreiber des WLAN Service?

Bei Nichteinhaltung der bestehenden Informations- und Speicherpflichten kann die Bundesnetzagentur Zwangsgelder bis zu einer Höhe von € 500.000,00 sowie Bußgelder für dann begangene Ordnungswidrigkeiten ebenfalls bis zu einer Höhe von € 500.000,00 festsetzen. Darüber hinaus sind auch die Vorschriften des Bundesdatenschutzgesetzes und der Datenschutzgesetze der Länder straf- bzw. ordnungsgeldbewährt.
Und schließlich ist bei fehlendem Außenschutz des WLAN-Netzes die Gefahr der Inanspruchnahme als Störer bei Urheberrechtsverletzungen oder ähnlichem gegeben.

Schützt die Abgabe der Dienstleistung an einen externen Betreiber vor Haftungsrisiken?

Die Abgabe der Dienstleistung an einen qualifizierten Dienstleister wie z. B. The Cloud schützt bei ordnungsgemäßer Erfüllung der vereinbarten Dienste vor einer Inanspruchnahme und reduziert das Haftungsrisiko deutlich. Vergleichbar ist dies mit dem Fall eines Schneeräumdienstes: Arbeitet dieser ordentlich, wird auch der Hauseigentümer nicht in Anspruch genommen werden können.

Wir möchten die Internetleitung des Unternehmens dem WLAN Betreiber zur Mitnutzung bereitstellen. Besteht dadurch ein erhöhtes Haftungsrisiko für das Unternehmen?

Im Idealfall sollte die Dienstleistung vollständig abgegeben werden. Durch die Mitbenutzung vorhandener Internetleitungen des Unternehmens besteht die Gefahr, dass auch das Unternehmen als Diensteanbieter gesehen wird und die Verpflichtungen selbst und direkt einhalten muss. Es erhöht sich also das Haftungsrisiko.

Wie ist vorzugehen, wenn wir als Anschlussinhaber zur Herausgabe von Verbindungsdaten aufgefordert werden.

Werden Sie als Anschlussinhaber zur Herausgabe von Verbindungsdaten aufgefordert, wenden Sie sich direkt an The Cloud.