

FSDZ RECHTSANWÄLTE & NOTARIAT AG  
ZUGERSTRASSE 76b  
CH-6340 BAAR  
Tel. ++ 41 41 727 60 80  
Fax. ++ 41 41 727 60 85  
faessler@fsdz.ch



#### Lukas Fässler

lic.iur.Rechtsanwalt<sup>1,2</sup>, Informatikexperte  
faessler@fsdz.ch

#### Carmen De la Cruz

Rechtsanwältin und Notarin<sup>1,2</sup>  
eidg. dipl. Wirtschaftsinformatikerin

Zugerstrasse 76b  
CH-6340 Baar  
Tel.: +41 41 727 60 80  
Fax: +41 41 727 60 85

[www.fsdz.ch](http://www.fsdz.ch)  
[sekretariat@fsdz.ch](mailto:sekretariat@fsdz.ch)  
UID: CHE-349.787.199 MWST



## IDENTIFIKATIONSPFLICHT FÜR PUBLIC WLAN

12.8.2019



Lukas Fässler, Rechtsanwalt & Informatikexperte

<http://www.fsdz.ch/team/faessler-lukas>

#### Partnerkanzleien:

##### **Böhni Rechtsanwälte GmbH**

**Roman Böhni**  
MLaw Rechtsanwalt,  
BSc Wirtschaftsinformatik  
Tel.: ++41 41 541 79 60  
[roman.boehni@boehnilaw.ch](mailto:roman.boehni@boehnilaw.ch)  
[www.boehnilaw.ch](http://www.boehnilaw.ch)

##### **de la cruz beranek Rechtsanwälte AG**

**Carmen De la Cruz**  
Rechtsanwältin und Notarin<sup>1,2</sup>  
eidg. dipl. Wirtschaftsinformatikerin  
[delacruz@delacruzberanek.com](mailto:delacruz@delacruzberanek.com)

##### **Nicole Beranek Zanon**

Rechtsanwältin und Notarin<sup>1,2</sup>  
[beranek@delacruzberanek.com](mailto:beranek@delacruzberanek.com)

Industriestrasse 7  
CH-6300 Zug  
Tel.: ++41 41 710 28 50  
Fax: ++41 41 710 90 76  
[www.delacruzberanek.com](http://www.delacruzberanek.com)  
UID: CHE-389.928.945 MWST

##### **Lichtsteiner Rechtsanwälte und Notare**

**Urs Lichtsteiner**  
lic. iur. Rechtsanwalt<sup>1,2</sup>, MSc (Stanford)  
[lichtsteiner@lilaw.ch](mailto:lichtsteiner@lilaw.ch)

Baarerstrasse 10, Postfach 7517  
CH-6302 Zug  
Tel.: +41 41 726 90 00  
Fax: +41 41 726 90 05  
[www.lilaw.ch](http://www.lilaw.ch)  
[info@lilaw.ch](mailto:info@lilaw.ch)  
UID: CHE-404.805.335 MWST

##### **Anwaltskanzlei Dr. Weltert**

**Hans M. Weltert**  
Dr. iur. Rechtsanwalt<sup>1,4</sup>  
[hans.weltert@raweltert.ch](mailto:hans.weltert@raweltert.ch)

##### **Matthias Heim**

lic.iur. Rechtsanwalt<sup>1,4</sup>  
[matthias.heim@raweltert.ch](mailto:matthias.heim@raweltert.ch)

##### **Michael Heim**

lic.iur. Rechtsanwalt<sup>1,4</sup>  
[michael.heim@raweltert.ch](mailto:michael.heim@raweltert.ch)

Bahnhofstrasse 10  
CH-5001 Aarau  
Tel.: +41 62 832 77 33  
Fax: +41 62 832 77 34  
[www.raweltert.ch](http://www.raweltert.ch)  
[info@raweltert.ch](mailto:info@raweltert.ch)  
UID: CHE-100.877.506 MWST

Baar, 12. August 2019

Von: Rechtsanwalt Lukas Fässler in Zusammenarbeit mit Rechtsanwalt  
Roman Böhni

## Identifikations-Pflichten beim Betrieb eines öffentlichen WLANs (Public-WLAN)

### 1. Zusammenfassender Überblick

Zugangspunkte zu einem Wireless Local Area Network (WLAN) in der Hotellerie gelten als öffentlich (Public WLAN). Der Betrieb eines Public WLANs ist in der Schweiz auch ohne Bewilligung grundsätzlich erlaubt. Eine Identifikationspflicht der Endbenutzer (vorliegend also der Hotelgäste) besteht lediglich für diejenigen Public WLANs, welche im Sinne des Gesetzgebers «**professionell betrieben**» werden. Der Betreiber ist auch nicht verpflichtet, den Zugang zu bestimmten Inhalten im Internet zu sperren.

### 2. Identifikationspflichten bei Public WLANs

#### 2.1. Gesetzliche Grundlagen

Die gesetzlichen Grundlagen für das Betreiben und Anbieten von Public WLAN-Dienstleistungen, insbesondere auch im Bereich der Hotellerie,

<sup>1</sup> Mitglied des Schweizerischen Anwaltsverbandes  
<sup>2</sup> Eingetragen im Anwaltsregister des Kantons Zug  
<sup>3</sup> Eingetragen im Anwaltsregister des Kantons Zürich  
<sup>4</sup> Eingetragen im Anwaltsregister des Kantons Aargau



bilden in der Schweiz einerseits das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) sowie die zugehörige Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF). Diese beiden Rechtstexte regeln primär die Überwachungspflichten des Post- und Fernmeldeverkehrs. Andererseits sind aber auch das Fernmeldegesetz (FMG) und die zugehörige Verordnung über Fernmeldedienste (FDV) einschlägig.

In Art. 19 Abs. 2 VÜPF hält der Bundesrat fest, dass keine generelle Identifikationspflicht der Endbenutzer (vorliegend also der Hotelgäste) an Public WLANs besteht. **Eine Identifikationspflicht besteht für diejenigen Public WLANs, die im Sinne des Gesetzgebers «professionell betrieben» werden.**

## 2.2. Identifikationspflicht für «professionell betriebene» Public WLANs in Hotelbetrieben

Sofern das im Hotel zur Verfügung gestellte Public WLAN durch einen meldepflichtigen Fernmeldediensteanbieter (FDA, z.B. Swisscom) oder einen auf öffentliche WLAN-Zugangspunkte spezialisierten IT-Dienstleister betrieben wird, müssen die Endbenutzer des Public WLAN (also die Hotelgäste), mit geeigneten Mitteln identifiziert werden. Dabei handelt es sich um eine **gesetzliche Pflicht, welcher der IT-Dienstleister zwingend nachkommen muss.** Darauf kann nicht verzichtet werden, auch nicht wenn der Hotelbetreiber dies ausdrücklich wünscht und bereit ist, eine Verzichtserklärung zu unterzeichnen

## 2.3. Keine Identifikationspflicht für selbstbetriebene Public WLANs in Hotelbetrieben

Sofern das Hotel das Public WLAN selber betreibt, muss es grundsätzlich keine Vorkehrungen treffen. In diesem Fall muss das Hotel die Identifikation der Endbenutzer (Hotelgäste) also nicht sicherstellen können. **ABER: Das Hotel muss auf Anordnung der Strafverfolgungsbehörden resp. aufgrund einer richterlichen Anordnung die bei ihm dennoch (freiwillig) vorhandenen resp. erhobenen Daten herausgeben resp. herausgeben können.** Wenn das Hotel also trotzdem eine Identifikation vornimmt und/oder anderweitige Nutzungsdaten erhebt resp. logged, muss es diese so aufbewahren, dass sie im Bedarfsfall den Strafverfolgungsbehörden ausgehändigt werden können. **Die Aufbewahrungsfrist dieser sogenannten Randdaten beträgt 6 Monate.**

Obwohl bei selbstbetriebenen Public WLANs weder eine Bewilligungspflicht noch eine Pflicht zur Identifikation der Nutzer besteht, soll an dieser Stelle noch auf nachfolgende Punkte hingewiesen werden:

- **Nachweisbare Einwilligung in Datenschutzerklärung (zwingend)**  
Wer in der Schweiz Systeme betreibt, die Personendaten (z.B. IP-Adressen, Namen, Telefonnummern etc.) bearbeiten (z.B. das Abspeichern von diesbezüglichen Daten in Logfiles), untersteht dem Schweizerischen Datenschutzgesetz und allenfalls auch ausländischen Datenschutzgesetzen (insb. DS-GVO für europäische Hotelkunden).



Die betroffenen Personen müssen vorgängig über ihre Rechte aufgeklärt werden und sie müssen ausdrücklich in die Datenbearbeitung einwilligen. Die Einwilligung muss nachweisbar sein (Protokollierung).

- **Nachweisbare Einwilligung in Nutzungsbedingungen (empfohlen)**  
Es wird empfohlen, die Nutzung des Public WLAN von der Zustimmung zu den Nutzungsbedingungen abhängig zu machen. Die Einwilligung sollte nachweisbar sein (Protokollierung). In den Nutzungsbedingungen sollten beispielsweise folgende Punkte geregelt werden:
  - Pflichten der Nutzer,
  - Hinweis auf Risiken und Gefahren bei der Nutzung des Public WLAN,
  - Haftungs- und Gewährleistungsausschlüsse des Betreibers,
  - Möglichkeit der Nutzungssperrung und des Rückgriffs auf Nutzer,
  - anwendbares Recht und
  - Gerichtsstand etc.
  
- **Beschränkung der Nutzung auf Hotelgäste (empfohlen)**
  
- **Starke Verschlüsselung, z.B. WPA2 (empfohlen)**
  
- **WLAN-Infrastruktur für Gäste von eigener (privater resp. betriebsinterner) Netzwerkinfrastruktur logisch trennen (empfohlen)**
  
- **Gäste untereinander durch Wireless-Isolation gegenseitig abschotten (empfohlen)**
  
- **Verschlüsselte und anonyme Kommunikation der Nutzer (insbesondere https://, VPN etc.) zulassen (empfohlen).**

FSDZ Rechtsanwälte & Notariat AG

Lukas Fässler  
Rechtsanwalt