Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Justice and Police FDJP

Post and Telecommunications Surveillance Service PTSS

Wireless LAN Information Sheet

Last revised on: 4 July 2018

Contents

Post and Telecommunications Surveillance Service PTSS
Fellerstrasse 15, 3003 Bern
www.li.admin.ch

1 Purpose of this Information Sheet

This information sheet defines the concept of "professionally operated public wireless LAN access point" within the meaning of Art. 19 para. 2 of the Ordinance on Post and Telecommunications Surveillance (VÜPF)[1] in relation to the obligation to identify end users. It explains the concept by providing examples.

It also describes the network coverage analysis procedure (Art. 64 VÜPF) and the procedure for conducting searches by antenna coverage area (Art. 66 VÜPF) for wireless LANs.

2 Context

Art. 21 para. 1 let. d of the Swiss Federal Act on Post and Telecommunications Surveillance (APTS)[2] lays down the obligation for telecommunications service providers (TSPs) to supply the Post and Telecommunications Surveillance Service (PTSS) with other telecommunications service data specified by the Federal Council allowing individuals to be identified. This obligation is described in detail for professionally operated public wireless LAN access points in Art. 19 para. 2 of the Ordinance on Post and Telecommunications Surveillance (VÜPF):

> Art. 19 para. 2 VÜPF
>
> "[2]For professionally operated public wireless LAN access points, TSPs must ensure that all end users are identified by suitable means."

In accordance with the principle of proportionality, the Federal Council's fully revised Ordinance on Post and Telecommunications Surveillance (VÜPF) does not contain a general obligation to identify end users at public wireless LAN access points so that, for example, private households and small businesses that give third parties access to their wireless LANs are not obliged to identify end users. Instead, the obligation to identify end users is restricted to "professionally operated" public wireless LAN access points (see Section 4.3).

3 Overview of the Different Types of Wireless LAN Access Points

The following three types of wireless LAN access points are relevant to this information sheet:

1. Professionally operated public wireless LAN access points;
2. Public wireless LAN access points that are operated non-professionally;
3. Non-public wireless LAN access points.

[1] Ordinance of 15 November 2017 on the Surveillance of Post and Telecommunications (SR 780.11). Entry into force: 1 March 2018.

[2] Federal Act of 18 March 2016 on Post and Telecommunications Surveillance (SR 780.1). Entry into force: 1 March 2018.

4 How to Identify a Professionally Operated Public Wireless LAN Access Point

For Art. 19 para. 2 VÜPF to be applicable, all three criteria below must be met:

1. It is a **wireless LAN access point;**
2. It is **public;**
3. It is **professionally operated**.

4.1 What is a Wireless LAN access point?

- It is a wireless access point providing access to a public telecommunications network (network access), which may be located in public or private areas.
- Network access is via a local radio network, which is usually based on one of the IEEE-802.11 standards (wireless LAN or WLAN).

4.2 When is a Wireless LAN access point considered public?

A wireless LAN access point is considered public when it provides network access to third parties. Whether or not network access is password-protected is irrelevant. “Third parties” is to be understood as other legal or natural persons.

Examples illustrating the difference between "public" and "non-public" wireless LAN access points:

- Public wireless LAN access points: at airports, at railway stations, at public transport stops, on public transport, in tourist accommodation establishments, in restaurants, in shops, in shopping centres, on public roads and in public squares;
- Non-public wireless LAN access points: where network access is available only to persons who are not considered third parties (e.g. employees or members of the household).

Public wireless LAN access points[3] are commonly referred to as WLAN hotspots, Wi-Fi®[4] hotspots, Wi-Fi®, or public wireless LANs (PWLANs).

[3] Public wireless LAN access points do not include TSP-operated wireless LAN services made available solely to TSP customers in connection with a different service (e.g. mobile or broadband subscriptions) such as UPC Wi-Free or Swisscom EAP-SIM (as at February 2018). Users of such TSP-operated wireless LAN services are identified as customers of the TSP.

[4] Wi-Fi® (also “WiFi”) is a registered trademark of Wi-Fi Alliance (www.wi-fi.org).

4.3 What is meant by "professionally operated"?

A public wireless LAN access point is "professionally operated" when it is operated by a legal or natural person ("wireless LAN specialist") who operates a number of public wireless LAN access points in multiple locations (i.e. not in the same location).

The term "same location" is defined as follows in accordance with Art. 2 of the Ordinance of 9 March 2007 on Telecommunications Services (OTS, SR 784.101.1):

1. Public wireless LAN access points are situated within the same building; or
2. Public wireless LAN access points are situated on a real property or on two adjacent or opposite real properties separated by a road, path, railway line or watercourse.

"Operate" is understood, in particular, as providing one or more of the following services for the public wireless LAN access point:

- Configuration management
- Remote or on-site maintenance
- Authentication, authorisation and accounting (AAA)
- Operation monitoring
- Software and firmware updates
- Capacity management
- Customer service and support

5 Identification

5.1 Who has an obligation to identify end users?

The obligation to identify end users rests with the TSP that operates, or arranges to operate, the public wireless LAN access point. The name under which Internet access is provided is also relevant, i.e. who is regarded as providing the public wireless LAN access point. The TSP may assign user identification to a third party, for example through outsourcing. If third parties are called upon for user identification, the provisions of Art. 23 VÜPF (subcontractors) are to be observed.

5.2 What is meant by "suitable means of identification”?

"Suitable means of identification" (also referred to as "indirect identification") are understood as implicit or simplified registration via trusted information allowing sufficient identification of end users.

These might include the following means:

- Access code sent to a mobile telephone by SMS and storage of MSISDN;
- Identification via credit card and storage of authorisation data;
- Identification via trusted data from roaming partners (e.g. WISPr or eduroam) and storage of authorisation data;
- Personal hotel room access code assigned to the guest at check-in;
- Identification via a valid airport boarding pass and storage of boarding pass data (e.g. a scanned boarding pass could generate a voucher [access code] for the wireless LAN);
- Identification via a frequent-flier card granting access to the lounge; storage of authorisation data.

6 Examples

6.1 Examples of professionally operated public wireless LAN access points

The following examples of professionally operated public wireless LAN access points are subject to mandatory verification of end user identity by suitable means.

Example	**Characteristics**	**Who has an obligation to verify the identity of end users?**
TSP-operated public wireless LAN	Operated by a TSP	TSP
Wireless LAN at a railway station or public transport stop or on public transport	Operated professionally	TSP providing the wireless LAN
Public wireless LAN at a catering establishment or hotel	Operated professionally	TSP providing the wireless LAN
Public wireless LAN at a museum or library or in a function room	Operated professionally	TSP providing the wireless LAN
Public wireless LAN in a town or municipality	Operated professionally	TSP providing the wireless LAN

6.2 Examples of wireless LAN access points that are not subject to mandatory verification of end user identity

The following examples of wireless LAN access points are not subject to mandatory verification of end user identity.

In some of the examples below, the characteristics of the wireless LAN access point will determine whether or not the access point is considered to be operated professionally and therefore subject to mandatory verification of end user identity.

Example	**Characteristics**	**Who has an obligation to verify the identity of end users?**
Guest wireless LAN in a company	Operated non-professionally	no one
"Open" private wireless LAN	Operated non-professionally	no one
Private guest wireless LAN	Operated non-professionally	no one
Non-professionally operated public wireless LAN at a restaurant or hotel	Operated non-professionally	no one
Non-professionally operated public wireless LAN at a museum or library or in a function room	Operated non-professionally	no one
Non-professionally operated public wireless LAN on a camping site	Operated non-professionally	no one

7 Searches by Antenna Coverage Area and Network Coverage Analysis for Wireless LANs

7.1 Network coverage analysis for wireless LANs

In accordance with Art. 64 VÜPF, network coverage analysis for the purpose of conducting searches by antenna coverage area as per Art. 66 VÜPF may now also be ordered for public wireless LAN access points. However, this only makes sense if the TSP operating the public wireless LAN access points is also able to perform a search by antenna coverage area for these. Unlike the already familiar network coverage analysis carried out for mobile radio cells, the output of which may also be expressed in the form of a coverage map, no coverage map is required for public wireless LAN access points. Instead, it is a matter of identifying the public wireless LAN access points that are most likely to cover a specific location (geographical coordinates or postal address), if necessary taking into account additional information such as time of day, day of the week, indoor vs. outdoor, or floor or section of a building. The authority issuing the surveillance order will share this information with the Post

and Telecommunications Surveillance Service, which will then forward it to the TSP along with the surveillance order.

The aim is to identify the public wireless LAN access points that are to be considered for a search by antenna coverage area as they may have provided access to the network at a given location, if necessary taking into account the additional information provided.

7.2 Searches by antenna coverage area for wireless LANs

In accordance with Art. 66 VÜPF, searches by antenna coverage area are now also possible for public wireless LAN access points. As with the already familiar searches by antenna coverage area conducted for mobile radio cells, this allows retroactive surveillance and concerns TSPs with full surveillance obligations in particular. TSPs with limited surveillance obligations are not obliged to store metadata and are therefore required only to provide the data at their disposal. The target identifier is the unique identifier (e.g. BSSID or location information in accordance with the TSP's internal identifiers) of the public wireless LAN access point. The surveillance order submitted to the TSP also specifies the period of time for which retroactive surveillance is required.