



# Notice « WLAN »

Version du :

4<sup>o</sup> juillet 2018

## Table des matières

<b>1</b>	<b>But du document .....</b>	<b>2</b>
<b>2</b>	<b>Contexte .....</b>	<b>2</b>
<b>3</b>	<b>Vue d'ensemble des types de points d'accès au réseau WLAN .....</b>	<b>2</b>
<b>4</b>	<b>Aspects à examiner pour déterminer s'il s'agit d'un point d'accès public au réseau WLAN exploité à titre professionnel.....</b>	<b>3</b>
4.1	Qu'est-ce qu'un point d'accès au réseau WLAN ? .....	3
4.2	À quelles conditions un accès au réseau WLAN est-il réputé public ?.....	3
4.3	Qu'entend-on par « exploité à titre professionnel » ? .....	4
<b>5</b>	<b>Identification .....</b>	<b>4</b>
5.1	À qui l'obligation d'identifier les utilisateurs finaux s'applique-t-elle ? .....	4
5.2	Qu'entend-on par « identifier par des moyens appropriés » ? .....	5
<b>6</b>	<b>Exemples.....</b>	<b>5</b>
6.1	Exemples de points d'accès publics au réseau WLAN exploités à titre professionnel .....	5
6.2	Exemples de points d'accès au réseau WLAN pour lesquels il n'y a pas d'obligation d'identifier les utilisateurs finaux.....	6
<b>7</b>	<b>Recherche par champ d'antenne et analyse de la couverture réseau dans le cas d'un réseau WLAN.....</b>	<b>6</b>
7.1	Analyse de la couverture réseau .....	6
7.2	Recherche par champ d'antenne .....	7

# 1 But du document

La présente notice explique et illustre, à l'aide d'exemples, ce qu'il faut entendre par « points d'accès publics au réseau WLAN » au sens de l'art. 19, al. 2, OSCPT<sup>1</sup> en lien avec l'obligation d'identifier les utilisateurs finaux.

Elle précise également les procédures de l'analyse de la couverture réseau (art. 64 OSCPT) et de la recherche par champ d'antenne (art. 66 OSCPT) en relation avec un réseau WLAN.

## 2 Contexte

Pour permettre d'identifier des personnes, l'art. 21, al. 1, let. d, LSCPT<sup>2</sup> impose aux fournisseurs de services de télécommunication (FST) de livrer au Service SCPT d'autres données, déterminées par le Conseil fédéral, concernant les services de télécommunication. Cette obligation est concrétisée à l'art. 19, al. 2, OSCPT pour les points d'accès publics au réseau WLAN qui sont exploités à titre professionnel.

Art. 19, al. 2, OSCPT

«<sup>2</sup> Les FST veillent à identifier par des moyens appropriés tous les utilisateurs finaux de points d'accès publics au réseau WLAN exploités à titre professionnel.»

Pour des raisons de proportionnalité, le Conseil fédéral n'a pas instauré, dans l'OSCPT entièrement révisée, une obligation générale d'identifier les utilisateurs finaux. Il s'agit d'éviter que des particuliers ou des petites entreprises qui mettent leur accès au réseau WLAN à la disposition de tiers ne soient eux aussi tenus d'identifier les utilisateurs finaux. Ce devoir d'identification est restreint aux seuls points d'accès publics au WLAN « exploités à titre professionnel » (voir ch. 0).

## 3 Vue d'ensemble des types de points d'accès au réseau WLAN

Aux fins de la présente notice, trois types de points d'accès sont pertinents :

1. les points d'accès publics au réseau WLAN exploités à titre professionnel,
2. les points d'accès publics au réseau WLAN qui ne sont pas exploités à titre professionnel, et
3. les points d'accès au réseau WLAN qui ne sont pas publics.

---

<sup>1</sup> Ordonnance du 15 novembre 2017 sur la surveillance de la correspondance par poste et télécommunication (**OSCPT**; RS **780.11**), entrée en vigueur le 1<sup>er</sup> mars 2018

<sup>2</sup> Loi fédérale du 18 mars 2016 sur la surveillance de la correspondance par poste et télécommunication (**LSCPT**; RS **780.1**), entrée en vigueur le 1<sup>er</sup> mars 2018

## 4 Aspects à examiner pour déterminer s'il s'agit d'un point d'accès public au réseau WLAN exploité à titre professionnel

Pour que l'art. 19, al. 2, OSCPT s'applique, les trois conditions ci-après doivent être remplies cumulativement :

1. il s'agit d'un **point d'accès** au réseau WLAN ;
2. celui-ci est **public** ;
3. il est **exploité à titre professionnel**.

### 4.1 Qu'est-ce qu'un point d'accès au réseau WLAN ?

- Il s'agit d'un point d'accès sans fil à un réseau public de télécommunication (accès au réseau) qui peut se trouver aussi bien dans des locaux publics que dans des locaux privés.
- L'accès au réseau se fait via un réseau radio local, fondé le plus souvent sur la norme IEEE-802.11 (Wireless LAN, WLAN).

### 4.2 À quelles conditions un accès au réseau WLAN est-il réputé public ?

Un accès au réseau WLAN est réputé public dès lors qu'il est mis à la disposition de tiers, que cet accès soit protégé ou non par un mot de passe. On entend par tiers toute autre personne physique ou morale.

Exemple de points d'accès « publics » et « non publics » au réseau WLAN :

- points d'accès publics : dans des aéroports, dans des gares, aux arrêts des transports publics, dans des véhicules des transports publics, dans des établissements hôteliers, dans des établissements de restauration, dans des magasins, dans des centres commerciaux, dans la rue et sur des places publiques
- points d'accès non publics : accessibles uniquement aux personnes qui ne sont pas considérées comme des tiers selon la définition donnée ci-dessus (par ex. collaborateurs, membres du ménage)

Appellations courantes pour désigner un point d'accès public au réseau WLAN<sup>3</sup> : hotspot WLAN, hotspot Wi-Fi®<sup>4</sup>, Wi-Fi®, Public Wireless LAN (PWLAN)

---

<sup>3</sup> Ne sont pas considérés comme des points d'accès publics des services WLAN exploités par des FST et qui ne sont disponibles que pour les clients de ce FST en lien avec une autre prestation (par ex. abonnement de téléphonie mobile ou abonnement haut débit), par ex. Wi-Free de UPC ou EAP-SIM de Swisscom (état : février 2018). Les usagers de ces services WLAN exploités par des FST sont identifiés en tant que clients du FST en question.

<sup>4</sup> Wi-Fi® (ou WiFi) est une marque déposée de la Wi-Fi Alliance ([www.wi-fi.org](http://www.wi-fi.org)).

## 4.3 Qu'entend-on par « exploité à titre professionnel » ?

Un point d'accès public au réseau WLAN est réputé être exploité à titre professionnel lorsque la personne physique ou morale qui l'exploite (spécialiste WLAN) exploite plusieurs accès publics sur des sites différents (c'est-à-dire qu'ils ne sont pas situés au même endroit).

L'expression « même endroit » est définie comme suit, en référence à l'art. 2 OST<sup>5</sup> :

1. les points d'accès publics au réseau WLAN se trouvent à l'intérieur du même bâtiment, ou
2. les points d'accès publics au réseau WLAN se trouvent sur un bien-fonds, sur deux biens-fonds contigus ou sur deux biens-fonds opposés, séparés par une route, une rue, un chemin, une ligne ferroviaire ou un cours d'eau.

Par « exploiter », il faut entendre notamment une ou plusieurs des prestations ci-après en relation avec le point d'accès public au réseau WLAN :

- gestion de configuration
- maintenance sur place ou à distance
- contrôle des accès, gestion des autorisations, décompte (protocole AAA, *Authentication Authorisation Accounting*)
- surveillance (monitorage) du bon fonctionnement
- actualisation des logiciels et micro-logiciels
- gestion de la capacité
- service et assistance clients

## 5 Identification

### 5.1 À qui l'obligation d'identifier les utilisateurs finaux s'applique-t-elle ?

L'obligation d'identifier les utilisateurs finaux s'applique au FST qui exploite ou fait exploiter le point d'accès public au réseau WLAN. À cet égard, le nom sous lequel l'accès à internet est proposé a aussi son importance. En d'autres termes, il importe de savoir qui se présente comme le fournisseur de l'accès public au réseau WLAN vis-à-vis des utilisateurs finaux. Le FST peut transférer l'obligation d'identification à des tiers (externalisation). Le recours à des tiers est soumis aux prescriptions de l'art. 23 OSCPT.

---

<sup>5</sup> Ordonnance du 9 mars 2007 sur les services de télécommunication (OST ; RS 784.101.1)

## 5.2 Qu'entend-on par « identifier par des moyens appropriés » ?

Un moyen d'identification approprié désigne l'enregistrement simplifié ou implicite de données dignes de confiance (*trusted*) permettant une identification suffisante de l'utilisateur final.

Moyens d'identification envisageables :

- code d'accès envoyé par SMS sur le téléphone mobile et enregistrement du MSISDN ;
- carte de crédit et enregistrement des données d'autorisation ;
- données dignes de confiance fournies par des partenaires d'itinérance (par ex. WISPr, eduroam) et enregistrement des données d'autorisation ;
- code d'accès individuel par chambre fourni par l'hôtel à ses clients lors de leur enregistrement ;
- à l'aéroport, carte d'embarquement valable et enregistrement des données d'embarquement (par ex. un bon [code d'accès] pour le WLAN est généré lors de la numérisation de la carte d'embarquement) ;
- carte de voyageur fréquent d'une compagnie aérienne qui donne accès aux salons privés, et enregistrement des données d'autorisation.

## 6 Exemples

### 6.1 Exemples de points d'accès publics au réseau WLAN exploités à titre professionnel

Pour les exemples ci-après de points d'accès publics au réseau WLAN, il y a obligation d'identifier les utilisateurs finaux par des moyens appropriés.

Exemple	Caractéristique	Qui a l'obligation d'identifier l'utilisateur final
WLAN public d'un FST	Exploité par le FST	FST
WLAN dans des gares, arrêts ou véhicules de transports publics	Exploité à titre professionnel	FST proposant le réseau WLAN
WLAN public dans des établissements hôteliers ou de restauration	Exploité à titre professionnel	FST proposant le réseau WLAN
WLAN public dans des musées, des bibliothèques, des salles accueillant des manifestations diverses	Exploité à titre professionnel	FST proposant le réseau WLAN
WLAN public dans des villes et des communes	Exploité à titre professionnel	FST proposant le réseau WLAN

## 6.2 Exemples de points d'accès au réseau WLAN pour lesquels il n'y a pas d'obligation d'identifier les utilisateurs finaux

Pour les exemples ci-après de points d'accès au réseau WLAN, il n'y a pas d'obligation d'identifier les utilisateurs finaux.

Dans certains des exemples ci-dessous, l'obligation d'identifier les utilisateurs finaux dépend de la caractéristique du réseau, c'est-à-dire s'il est exploité ou non à titre professionnel.

Exemple	Caractéristique	Qui a l'obligation d'identifier l'utilisateur final
WLAN pour les visiteurs dans une entreprise	Pas exploité à titre professionnel	Personne
WLAN privé « ouvert »	Pas exploité à titre professionnel	Personne
WLAN privé destiné aux visiteurs	Pas exploité à titre professionnel	Personne
WLAN public qui n'est pas exploité à titre professionnel dans un établissement hôtelier ou de la restauration	Pas exploité à titre professionnel	Personne
WLAN public qui n'est pas exploité à titre professionnel dans des musées, des bibliothèques, des salles accueillant des manifestations diverses	Pas exploité à titre professionnel	Personne
WLAN public qui n'est pas exploité à titre professionnel dans un camping	Pas exploité à titre professionnel	Personne

## 7 Recherche par champ d'antenne et analyse de la couverture réseau dans le cas d'un réseau WLAN

### 7.1 Analyse de la couverture réseau

L'art. 64 OSCPT autorise désormais une analyse de la couverture réseau préalablement à une recherche par champ d'antenne selon l'art. 66 OSCPT également pour les points d'accès publics au réseau WLAN. Cette mesure n'a toutefois de sens que si le FST qui exploite le point d'accès public au réseau WLAN est aussi en mesure d'exécuter la recherche par champ d'antenne pour le point d'accès en question. Les analyses traditionnelles de la couverture réseau de cellules de radiocommunication peuvent aussi être représentées sous la forme de cartes de couverture. Pour les points d'accès publics au réseau WLAN en revanche, il n'est pas possible d'établir une telle carte. Dans ce type de mesure, il s'agit d'identifier les points d'accès publics au réseau WLAN le plus susceptibles de couvrir une localisation donnée

(coordonnées géographiques ou adresse postale). Le cas échéant, il faut intégrer dans la recherche des données supplémentaires (par ex. heure du jour, conditions météorologiques, jour de la semaine, localisation à l'intérieur ou à l'extérieur d'un bâtiment, étage, partie du bâtiment). L'autorité qui ordonne l'analyse communique ces indications au Service SCPT, qui les transmet ensuite au FST avec le mandat.

Le but est de déterminer, au besoin à l'aide de données supplémentaires, quels sont les points d'accès publics au réseau WLAN qui entrent en ligne de compte pour une recherche par champ d'antenne, car susceptibles d'avoir permis une connexion au réseau.

## **7.2 Recherche par champ d'antenne**

L'art. 66 OSCPT permet désormais d'effectuer une recherche par champ d'antenne également pour les points d'accès publics au réseau WLAN. Il s'agit, comme pour les recherches par champ d'antenne traditionnelles concernant des cellules de radiocommunication, d'une surveillance rétroactive. Cette mesure concerne en priorité les FST qui ont des obligations complètes en matière de surveillance. En effet, comme les FST qui ont des obligations restreintes ne sont pas tenus de conserver les données secondaires, ils ne livrent que les données dont ils disposent le cas échéant. L'identifiant à surveiller est l'identifiant (par ex. BSSID ou les données de localisation selon les désignations internes du FST) du point d'accès public au réseau WLAN. Il y a lieu d'indiquer dans le mandat de surveillance qui est transmis au FST l'intervalle sur lequel porte la surveillance rétroactive.