Wi-Fi Public : Guide de Bonnes Pratiques

“

Wi-Fi public : un simple service… ou une vraie responsabilité légale ?

En France, proposer un accès Internet au public (Wi-Fi **ou filaire**) n’est pas neutre juridiquement.
Toute organisation doit **tracer les connexions d’équipements qui ne lui appartiennent pas**.

👉 Cela concerne aussi bien les entreprises que les collectivités, médiathèques ou ERP.

“

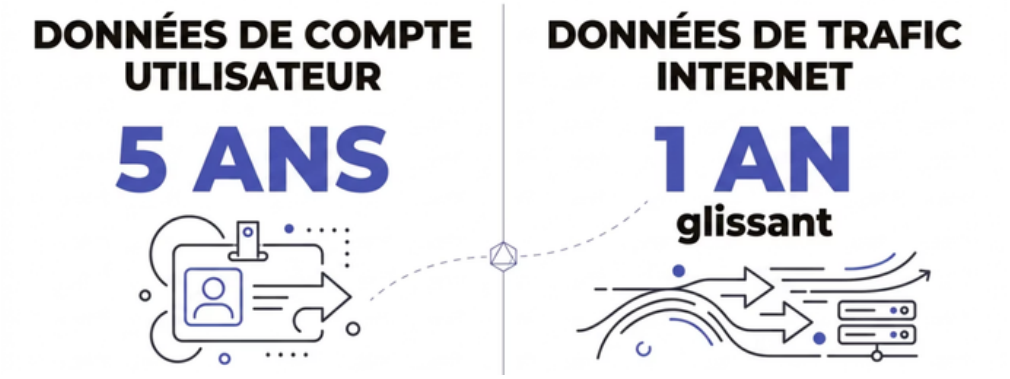
Pourquoi c'est IMPORTANT

La législation française impose à toute organisation proposant un accès Internet public de tracer l'activité des appareils qui ne lui appartiennent pas. Cette réglementation s'applique tant aux connexions WiFi qu'aux connexions filaires. Le non-respect de ces obligations expose les mandataires sociaux à des responsabilités pénales importantes.

Au-delà du **Code des Postes et Communications Électroniques** de 2021 (Articles L34-1 et R10-13), les organisations doivent également respecter le **Règlement Général sur la Protection des Données** européen concernant la collecte et le traitement des données personnelles.

Ce que la LOI IMPOSE

Exigences de conservation des données selon le CPCE:



Deux catégories de données doivent être conservées selon des durées distinctes :

1. Les **données de compte utilisateur**, comprenant l'adresse MAC considérée comme donnée personnelle, doivent être stockées pendant 5ans.

Les données de compte utilisateur sont principalement des données d'identification et de gestion du service, par exemple :

- nom et prénom
- adresse e-mail
- identifiant de connexion
- mot de passe (haché)
- numéro de téléphone
- préférences utilisateur
- historique de connexion ou d'utilisation du service.

2. Les **données de trafic Internet** doivent être conservées pendant 1an, avec effacement automatique au 366ème jour. L'adresse MAC appartient aux deux catégories, d'où sa double classification.

Sur la base de l'article L.34-1 CPCE et de sa doctrine d'application, les données de trafic internet comprennent notamment :

- Données d'identification technique de l'utilisateur
  - Identité civile de l'abonné ou de l'utilisateur (nom, prénom, adresse)
  - Identifiant de connexion ou identifiant technique attribué par l'opérateur
  - Numéro de client ou de contrat

Ces données permettent de rattacher une communication à un utilisateur déterminé.

- Données liées aux connexions internet
  - Adresse IP attribuée à l'utilisateur
  - Ports de connexion source et destination
  - Protocole utilisé (TCP, UDP, etc.)
  - Fournisseur d'accès ou service utilisé

Elles décrivent comment la communication circule sur le réseau.

- Données temporelles
    - Date et heure de début de connexion
    - Date et heure de fin
    - Durée de la communication ou de la session

Elles permettent la reconstitution chronologique des usages.

- Données de localisation technique
    - Localisation du point d'accès au réseau
    - Données permettant d'identifier le terminal ou le point de terminaison
    - Cellule réseau ou zone technique (selon la technologie utilisée)

Il s'agit d'une localisation technique, non du déplacement précis de la personne.

Critère	**Données de compte utilisateur (RGPD)**	**Données de trafic internet (CPCE)**
Texte juridique	Règlement (UE) 2016/679 (RGPD), art. 4 §1	Code des postes et communications électroniques, art. L.34-1
Définition juridique	Toute information se rapportant à une personne physique identifiée ou identifiable	Données relatives aux communications électroniques, nécessaires à leur traçabilité
Nature des données	Données déclaratives et fonctionnelles	Données techniques (métadonnées)
Lien avec l'utilisateur	Identification directe ou indirecte de la personne	Rattachement technique d'une communication à un utilisateur

Critère	Données de compte utilisateur (RGPD)	Données de trafic internet (CPCE)
Contenu des échanges	Non concerné	Strictement exclu
Principe de conservation	Conservation limitée, proportionnée à la finalité	Effacement/anonymisation de principe
Obligation légale de conservation	Aucune obligation générale	Conservation obligatoire 1an glissant
Durée de conservation	Déterminée par le responsable de traitement	Fixée par la loi et ses décrets d'application
Logique juridique dominante	Protection des droits et libertés individuelles	Protection de la sécurité publique et du fonctionnement des réseaux

Les données de compte utilisateur relèvent d'un traitement volontaire de service, soumis aux principes classiques du RGPD (finalité, minimisation, droits des personnes).
Les données de trafic internet, au sens du CPCE, relèvent d'un régime dérogatoire, fondé sur la nécessité technique et la sécurité publique, avec des obligations légales de conservation indépendantes du consentement.

👉 Les données de compte utilisateur sont des données RGPD, mais elles basculent sous le régime CPCE dès lors qu'elles sont utilisées pour identifier ou tracer une communication électronique.

En cas de non-conformité, la responsabilité pénale peut remonter jusqu'aux dirigeants.

Risques REQUISITIONS JUDICIAIRES

Réquisitions les plus fréquentes

Fraudes à la carte bancaire via Wi-Fi public.

Risque juridique

Si l'établissement ne peut prouver l'absence d'implication, le matériel informatique peut être saisi.

Conséquence

Coupure totale du service proposé (Internet).

Les réquisitions judiciaires les plus fréquentes concernent des fraudes à la carte bancaire, où des personnes utilisent des cartes volées via des hotspots WiFi publics. Ces réquisitions arrivent généralement dans la semaine suivant l'infraction. Si l'établissement ne peut prouver qu'aucun membre du personnel n'est impliqué, faute de données de traçabilité conformes, les autorités peuvent saisir l'ensemble du matériel informatique , entraînant une coupure totale d'Internet.

Pourquoi les portails Wi-Fi classiques ne SUFFISENT PAS ?

La technologie complique la traçabilité

Les adresses MAC sont désormais virtuelles et changent régulièrement pour des raisons de protection des données analytiques. Sur les appareils iOS, cette modification intervient environ toutes les deux semaines, tandis que sur Android elle s'effectue environ toutes les six semaines. Cette évolution répond aux préoccupations de confidentialité soulevées par Apple et Google concernant le suivi des utilisateurs**.**

La conformité RGPD & cadre légal européen Vs Loi Française

- Ne respectent pas les durées de conservation françaises.
- Ne distinguent pas correctement logs utilisateurs / trafic.
- Limitent la conservation des données à quelques semaines.

Passez à l'ACTION

Le **Wi-Fi public** n'est pas qu'une question de connectivité, c'est un sujet **juridique**, de **sécurité**... et de **responsabilité**.

> ***Nous serions ravis de vous accompagner sur le choix des bons outils pour assurer votre conformité !***

Contactez notre équipe commerciale: sales@connectdata.fr

Clause de non-responsabilité et réserve juridique

Le présent document est fourni à titre informatif et vise à apporter un éclairage technique et général sur les obligations relatives à l'utilisation des réseaux Wi-Fi en France.

Il ne constitue en aucun cas un conseil juridique, ni une consultation juridique formelle. Les informations et analyses présentées reposent sur une interprétation des textes législatifs et réglementaires en vigueur à la date de rédaction, laquelle est susceptible d'évoluer ou de faire l'objet d'interprétations divergentes par les autorités compétentes.

Compte tenu de la diversité des contextes d'application et des situations propres à chaque organisation, il appartient au lecteur de s'assurer de la conformité de ses pratiques avec la réglementation applicable, le cas échéant en sollicitant l'avis d'un conseil juridique qualifié.

En conséquence, Connect Data ne saurait être tenue responsable des décisions prises, des actions menées ou des conséquences résultant de l'utilisation des informations contenues dans ce document.

Les recommandations formulées doivent être considérées comme des éléments d'aide à la décision et doivent, le cas échéant, être adaptées au contexte spécifique de chaque organisation.