

# Bloquer WhatsApp sur le WiFi de l'entreprise : est-ce autorisé au Luxembourg ?

## Réponse courte

L'employeur peut **bloquer techniquement WhatsApp** sur le réseau WiFi de l'entreprise dans le cadre de son pouvoir de direction sur les outils informatiques. Le **blocage est licite** s'il poursuit une finalité légitime (sécurité des données, productivité, prévention des fuites), s'il est **proportionné** et si les salariés en sont **préalablement informés** via la charte informatique. La mesure doit être inscrite au registre des traitements et, dans les entreprises dotées d'une délégation, faire l'objet d'une **consultation préalable** (art. [L.414-1](#) du Code du travail).

Le blocage d'applications grand public comme WhatsApp sur le réseau professionnel n'est pas assimilable à une surveillance individuelle des salariés : il s'agit d'une **mesure technique collective** de configuration réseau. En revanche, l'employeur doit veiller à ne pas basculer dans un contrôle excessif de la vie privée des salariés, notamment si le blocage s'étend aux appareils personnels connectés au WiFi dans le cadre d'un BYOD. Une alternative consiste à proposer un **WiFi invité séparé** pour les usages personnels, sans filtrage.

## Définition

Le **blocage applicatif** consiste à empêcher, via le pare-feu ou le proxy de l'entreprise, l'accès à certaines applications ou services web depuis le réseau de l'entreprise. Il peut cibler des applications spécifiques (WhatsApp, Messenger, Telegram), des catégories de sites (streaming, réseaux sociaux) ou des protocoles particuliers (torrent, VPN). Au Luxembourg, cette pratique relève du pouvoir de direction de l'employeur encadré par l'article [L.261-1](#) du Code du travail sur le contrôle des outils informatiques et par le RGPD pour ses implications sur le traitement des données de connexion.

## Questions fréquentes

### Faut-il informer les salariés du blocage de WhatsApp ?

Oui, les salariés doivent être préalablement informés via la charte informatique. La mesure doit être inscrite au registre des traitements et faire l'objet d'une consultation préalable de la délégation du personnel selon l'article [L.414-1](#) du Code du travail.

### Faut-il prévoir un WiFi invité séparé pour les usages personnels ?

Oui, il est recommandé de proposer un réseau WiFi invité séparé sans filtrage pour les usages personnels des salariés et visiteurs. Cette alternative respecte l'équilibre entre droit de l'employeur et respect de la vie privée au travail.

### Le blocage de WhatsApp est-il une surveillance des salariés ?

Non, le blocage d'applications grand public sur le réseau professionnel n'est pas assimilable à une surveillance individuelle. Il s'agit d'une mesure technique collective de configuration réseau, qui doit néanmoins respecter les principes du RGPD.

### Peut-on bloquer WhatsApp sur le WiFi de l'entreprise au Luxembourg ?

Oui, l'employeur peut bloquer techniquement WhatsApp sur le réseau WiFi dans le cadre de son pouvoir de direction. Le blocage est licite s'il poursuit une finalité légitime (sécurité, productivité), s'il est proportionné et si les salariés en sont informés.

### Peut-on journaliser les tentatives d'accès bloquées ?

Il convient d'éviter toute journalisation individuelle des tentatives d'accès bloquées, sauf justification précise et proportionnée. Une telle collecte constituerait une surveillance au sens de l'article L.261-1 du Code du travail luxembourgeois.

### Quelles obligations RGPD pour le blocage applicatif ?

L'inscription au registre des traitements (article 30 RGPD) est requise si le blocage implique un traitement de données de connexion. Une AIPD peut être nécessaire si le blocage s'accompagne d'un suivi individuel des tentatives d'accès.

## Conditions d'exercice

Le blocage de WhatsApp sur le WiFi d'entreprise n'est licite que si plusieurs conditions cumulatives tirées du RGPD et du Code du travail luxembourgeois sont respectées.

Condition	Détail
<b>Finalité légitime</b>	Sécurité informatique, prévention des fuites de données, productivité ou conformité sectorielle (ex : un cabinet d'avocats bloque WhatsApp pour éviter l'exfiltration de documents clients confidentiels)
<b>Proportionnalité</b>	Mesure adaptée au risque réel, pas de blocage excessif par principe
<b>Information préalable</b>	Charte informatique remise au salarié ou règlement intérieur mentionnant le blocage
<b>Consultation délégation</b>	Avis préalable de la délégation du personnel (art. <a href="#">L.414-1</a> )
<b>Registre des traitements</b>	Inscription de la mesure si elle implique un traitement de données de connexion
<b>AIPD éventuelle</b>	Analyse d'impact si le blocage s'accompagne d'un suivi individuel des tentatives
<b>Non-discrimination</b>	Application uniforme à tous les salariés, sans ciblage individuel

## Modalités pratiques

La mise en place d'un blocage de WhatsApp sur le WiFi d'entreprise commence par une analyse de la finalité, se poursuit par la rédaction ou la mise à jour de la charte informatique et l'information des salariés, puis par la configuration technique et la journalisation encadrée des tentatives d'accès.

Étape	Détail
<b>Analyse de besoin</b>	Justifier la finalité (sécurité, productivité, secteur réglementé)
<b>Charte informatique</b>	Mise à jour pour inclure la liste des applications bloquées et la justification
<b>Consultation délégation</b>	Avis préalable recueilli et documenté
<b>Configuration réseau</b>	Blocage applicatif via pare-feu, proxy ou DNS filtering
<b>Information salariés</b>	Communication claire avant l'activation du blocage
<b>WiFi invité</b>	Réseau séparé sans filtrage pour les appareils personnels des salariés et visiteurs
<b>Journalisation minimale</b>	Logs anonymisés ou agrégés, pas de suivi individuel par défaut

## Pratiques et recommandations

**Distinguer** le blocage collectif (mesure de configuration réseau licite) de la surveillance individuelle (qui relève de l'article [L.261-1](#) et nécessite des garanties renforcées) pour éviter tout grief de contrôle excessif.

**Proposer** un réseau WiFi invité séparé sans filtrage pour les usages personnels des salariés, afin de respecter l'équilibre entre droit de l'employeur et respect de la vie privée au travail.

**Documenter** la finalité du blocage dans la charte informatique et le registre des traitements pour pouvoir la justifier en cas de contrôle de la CNPD ou de contestation par un salarié.

**Consulter** la délégation du personnel avant toute mise en place ou modification du dispositif, car cette consultation est obligatoire pour les mesures affectant les conditions de travail (art. [L.414-1](#)).

**Éviter** toute journalisation individuelle des tentatives d'accès bloquées, sauf justification précise et proportionnée, car une telle collecte constituerait une surveillance au sens de l'article [L.261-1](#).

## Cadre juridique

Référence	Objet
<b>Art. <a href="#">L.261-1</a> Code du travail</b>	Contrôle des outils informatiques et surveillance des salariés
<b>Art. <a href="#">L.414-1</a> et s. Code du travail</b>	Information et consultation de la délégation du personnel
<b>RGPD, art. 5 et 6</b>	Principes de licéité, finalité et minimisation
<b>RGPD, art. 30</b>	Registre des activités de traitement
<b>RGPD, art. 35</b>	Analyse d'impact relative à la protection des données
<b>Loi du 1er août 2018</b>	Transposition nationale du RGPD

Le blocage de WhatsApp relève du pouvoir de direction de l'employeur et n'est pas interdit par le droit luxembourgeois, à condition d'être transparent, proportionné et documenté. La CNPD considère que les mesures collectives de configuration réseau sont moins intrusives qu'un contrôle individuel, mais elles doivent néanmoins respecter les principes du RGPD.

Les contenus sont rédigés et mis à jour régulièrement à partir de sources officielles. Leur usage ne remplace pas une consultation juridique et doit être validé par un professionnel du droit.