

WhatsApp et Messenger en entreprise : quelles règles RGPD ?

Réponse courte

L'usage de **WhatsApp** ou **Messenger** pour communiquer avec les salariés n'est **pas interdit par principe**, mais il est **fortement déconseillé** pour toute communication contenant des données personnelles. Ces applications grand public posent des problèmes de **base légale**, de **transferts hors Union européenne**, de **minimisation** et de **confidentialité** au regard du RGPD et des orientations de la **CNPD**.

L'employeur qui souhaite malgré tout recourir à ces outils doit limiter leur usage à des **messages opérationnels non sensibles** (rappels d'horaires, informations générales), obtenir le **consentement** du salarié et disposer d'une **alternative équivalente** pour ceux qui refusent. Pour les données sensibles (paie, santé, contrat), un **outil professionnel sécurisé** est impératif.

Définition

Les **messageries instantanées grand public** telles que WhatsApp ou Messenger sont des services de communication en ligne conçus pour un usage personnel, exploités par des sociétés établies hors de l'Union européenne. Elles reposent sur la collecte de métadonnées et l'identification par numéro de téléphone ou compte social. Leur utilisation professionnelle soulève des enjeux de protection des données, car elle implique un transfert de coordonnées vers le prestataire et un partage de contenu qui échappe partiellement au contrôle de l'employeur.

Questions fréquentes

Faut-il mentionner WhatsApp dans la charte informatique ?

Oui, les règles d'usage des messageries grand public doivent figurer dans la charte informatique annexée au règlement intérieur. La charte rappelle notamment l'interdiction d'envoyer des données RH sensibles via ces outils non sécurisés.

Peut-on envoyer des bulletins de paie par WhatsApp ?

Non, l'envoi de bulletins, certificats médicaux ou données contractuelles via WhatsApp ou Messenger doit être interdit dans la charte informatique. Pour les données sensibles (paie, santé, contrat), un outil professionnel sécurisé est impératif.

Peut-on utiliser WhatsApp ou Messenger en entreprise au Luxembourg ?

L'usage n'est pas interdit par principe mais fortement déconseillé pour toute communication contenant des données personnelles. Ces applications grand public posent des problèmes de base légale, transferts hors UE, minimisation et confidentialité au regard du RGPD.

Quel consentement requis pour utiliser WhatsApp au travail ?

L'employeur doit recueillir le consentement explicite du salarié avant d'utiliser son numéro personnel pour des communications professionnelles. Ce consentement doit être documenté et une alternative équivalente fournie à tout salarié refusant.

Quelles alternatives professionnelles à WhatsApp recommander ?

Il convient de privilégier des outils professionnels conformes au RGPD comme Teams, Slack Enterprise ou des solutions européennes pour toute communication contenant des données personnelles structurées. Ces outils offrent un contrôle des accès et une journalisation.

Quels risques RGPD pose WhatsApp en entreprise ?

Les risques concernent le transfert de coordonnées hors UE, l'absence de base légale claire, la collecte de métadonnées par le prestataire et le partage de contenu qui échappe au contrôle de l'employeur. La CNPD recommande des solutions européennes.

Conditions d'exercice

WhatsApp et Messenger ne sont tolérés que pour des messages opérationnels non sensibles, avec consentement documenté du salarié et alternative professionnelle en cas de refus.

Condition	Détail
Base légale	Consentement ou intérêt légitime documenté (art. 6 RGPD)
Minimisation	Pas de données sensibles, pas de pièces jointes RH confidentielles
Information	Notice explicite au salarié sur l'usage et les risques
Alternative	Canal équivalent disponible en cas de refus
Transferts	Vérification des garanties pour les transferts hors UE
Séparation vie privée	Pas d'usage en dehors des horaires de travail sans accord

Modalités pratiques

L'usage de WhatsApp ou Messenger pour échanger avec les salariés exige une analyse de risque préalable, des règles inscrites dans la charte informatique, une notice d'information dédiée et l'usage d'un numéro professionnel distinct.

Étape	Détail
Analyse de risque	Identification des communications concernées et des données traitées
Charte interne	Règles d'usage inscrites dans la charte informatique
Information salariés	Notice dédiée, acceptation documentée
Numéro professionnel	Utilisation d'un numéro dédié, pas d'appareil personnel du RH
Journalisation	Conservation raisonnée des échanges pour traçabilité
Réévaluation	Revue annuelle de la solution et des alternatives disponibles

Pratiques et recommandations

Privilégier des outils professionnels conformes au RGPD (Teams, Slack Enterprise, solutions européennes) pour toute communication contenant des données personnelles structurées.

Limiter strictement l'usage de WhatsApp ou Messenger à des messages opérationnels généraux, sans contenu sensible ni pièce jointe contenant des données RH.

Recueillir le consentement explicite du salarié avant d'utiliser son numéro personnel pour des communications professionnelles et documenter ce consentement.

Fournir une alternative équivalente à tout salarié refusant l'usage de ces applications, sans conséquence défavorable sur sa situation.

Rappeler dans la charte informatique que l'envoi de bulletins, certificats médicaux ou données contractuelles via ces outils est interdit.

Cadre juridique

Les règles applicables découlent principalement du RGPD et de la jurisprudence CNPD.

Référence	Objet
Art. 5 RGPD	Licéité, minimisation, limitation de la conservation
Art. 6 RGPD	Bases légales du traitement
Art. 13 RGPD	Information des personnes concernées
Art. 32 RGPD	Sécurité appropriée au risque
Art. 44 à 49 RGPD	Transferts de données hors UE
Loi du 1er août 2018	Régime national, pouvoirs de la CNPD
Art. <u>L.261-1</u> Code du travail	Surveillance des salariés, information préalable

La CNPD invite les employeurs à privilégier des solutions professionnelles européennes et à considérer WhatsApp comme un canal de communication informel. Le Comité européen de la protection des données souligne les risques liés aux transferts internationaux et aux fonctionnalités de métadonnées de ces applications.

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.