Que faire si un salarié utilise une messagerie non sécurisée pour des données RH ?

Réponse courte

L'usage par un salarié d'une **messagerie personnelle non sécurisée** pour envoyer ou recevoir des données RH engage la responsabilité de l'employeur en tant que **responsable du traitement** au sens du RGPD. Il s'agit potentiellement d'une **violation de confidentialité** devant être évaluée et, le cas échéant, **notifiée à la CNPD** dans les 72 heures.

L'employeur doit **rappeler le cadre** à l'intéressé, **mettre à disposition un canal professionnel sécurisé** et documenter la démarche. Selon la gravité, une **sensibilisation**, un **avertissement** ou une **sanction disciplinaire** proportionnée peuvent être envisagés. La **charte informatique** doit prévoir explicitement ce type de situation et sa prévention.

Définition

Une **messagerie non sécurisée** désigne tout canal de communication électronique ne garantissant pas la confidentialité, l'intégrité et la traçabilité des échanges : messagerie personnelle grand public, compte email privé, application non professionnelle. L'utilisation d'un tel canal pour transmettre des données RH (bulletins, contrats, certificats médicaux, coordonnées) constitue un risque de fuite de données au sens du RGPD et expose tant le salarié que l'employeur à des conséquences juridiques et disciplinaires.

Questions fréquentes

Comment prévenir l'usage de messageries non sécurisées ?

Il faut mettre à disposition un outil de messagerie professionnelle sécurisé et ergonomique, former régulièrement les salariés et inclure dans la charte informatique une clause explicite interdisant l'envoi de données RH via des messageries personnelles.

Faut-il documenter l'incident même s'il est résolu rapidement ?

Oui, chaque incident doit être inscrit au registre des violations, même résolu rapidement, pour démontrer la vigilance de l'entreprise. Cette documentation est exigée par l'article 33.5 du RGPD au titre du principe d'accountability.

Faut-il sanctionner systématiquement le salarié fautif ?

Non, il convient de privilégier une approche pédagogique avant toute sanction disciplinaire, sauf en cas de récidive, mauvaise foi ou préjudice avéré. La sanction doit rester proportionnée et conforme aux articles L.124-1 du Code du travail.

L'usage d'une messagerie personnelle constitue-t-il une violation RGPD ?

Oui, il s'agit potentiellement d'une violation de confidentialité au sens de l'article 4.12 du RGPD. Elle doit être évaluée et, le cas échéant, notifiée à la CNPD dans les 72 heures si le risque pour les droits du salarié est avéré.

Que faire si un salarié utilise une messagerie personnelle pour des données RH ?

L'employeur doit rappeler le cadre, mettre à disposition un canal professionnel sécurisé et documenter la démarche. Selon la gravité, une sensibilisation, un avertissement ou une sanction disciplinaire proportionnée peuvent être envisagés, conformément à la charte informatique.

Qui est responsable en cas d'usage abusif d'une messagerie par un salarié ?

L'employeur reste responsable du traitement au sens du RGPD, même lorsque l'incident résulte d'une initiative isolée d'un salarié. La CNPD peut considérer l'absence de charte claire et de formation comme une défaillance organisationnelle aggravante.

Conditions d’exercice

L'utilisation d'une messagerie non sécurisée par un salarié est qualifiée de violation potentielle au sens de l'art. 4.12 RGPD et peut imposer une notification à la CNPD dans les 72 heures si le risque pour les droits des personnes est avéré.

Condition	Détail
Qualification	Violation potentielle de confidentialité au sens de l'art. 4.12 RGPD
Évaluation du risque	Analyse de la sensibilité et du volume des données
Notification CNPD	72 heures si risque avéré pour les droits du salarié
Information	Information du salarié concerné si risque élevé
Sanction éventuelle	Proportionnée, documentée, conforme à la charte
Mesure corrective	Mise en place immédiate d'un canal sécurisé alternatif

Modalités pratiques

Dès la détection, l'employeur doit confiner les données, inscrire l'incident au registre des violations et notifier la CNPD sous 72 heures si un risque pour le salarié est avéré.

Étape	Détail
Détection	Signalement par un collègue, audit IT ou incident de sécurité
Entretien	Échange avec le salarié pour comprendre le contexte
Analyse	Évaluation du type et du volume de données exposées
Confinement	Suppression des données sur la messagerie personnelle
Registre	Inscription de l'incident dans le registre des violations
Mesure corrective	Rappel des règles et formation si nécessaire

Pratiques et recommandations

Mettre à disposition des salariés un outil de messagerie professionnelle sécurisé et ergonomique, car l'absence de solution pratique pousse aux contournements.

Former régulièrement les salariés aux règles de sécurité des données RH et aux canaux autorisés, en insistant sur les risques liés aux messageries personnelles.

Inclure dans la charte informatique une clause explicite interdisant l'envoi de données RH via des messageries personnelles, avec rappel des sanctions encourues.

Documenter chaque incident dans le registre des violations, même lorsqu'il est résolu rapidement, pour pouvoir démontrer la vigilance de l'entreprise.

Privilégier une approche pédagogique avant toute sanction disciplinaire, sauf en cas de récidive, de mauvaise foi ou de préjudice avéré.

Cadre juridique

Les règles applicables combinent RGPD, loi nationale et droit du travail.

Référence	Objet
Art. 5 RGPD	Principes de confidentialité et d'intégrité
Art. 32 RGPD	Sécurité du traitement
Art. 33 RGPD	Notification à la CNPD dans les 72 heures
Art. 4.12 RGPD	Définition de la violation de données
Loi du 1er août 2018	Régime national et rôle de la CNPD
Art. L.261-1 Code du travail	Cadre de la surveillance des salariés
Art. L.124-1 Code du travail	Cadre général des sanctions disciplinaires

La CNPD insiste sur la responsabilité première de l'employeur, même lorsque l'incident résulte d'une initiative isolée d'un salarié. L'absence de charte claire et de formation peut être considérée comme une défaillance organisationnelle et alourdir la sanction en cas de contrôle.