La transmission de données sociales par email non sécurisé est-elle autorisée ?

Réponse courte

La transmission de données sociales par email non sécurisé n'est pas automatiquement interdite, mais elle doit être **proportionnée au risque** présenté par les données transmises (Art. 32 RGPD). Pour les données ordinaires (rémunération, carrière, identité), un email professionnel standard peut être acceptable avec des mesures d'accès contrôlées. En revanche, pour les **données sensibles** (santé, appartenance syndicale, infractions — Art. 9 RGPD), des mesures de sécurité renforcées sont obligatoires : chiffrement de bout en bout, plateformes RH sécurisées ou transmission sécurisée.

L'employeur doit mettre en place des mesures techniques et organisationnelles appropriées et documenter les choix de sécurité adoptés. En cas de violation de données résultant d'une transmission non sécurisée, la responsabilité de l'employeur est engagée — notification à la CNPD dans les 72 heures si risque pour les droits des personnes concernées (Art. 33 RGPD).

Définition

Les **données sociales** des salariés regroupent les informations traitées dans le cadre de la relation de travail : données d'identification, rémunération, carrière, absences, évaluations. Parmi ces données, certaines sont des **données ordinaires** (Art. 6 RGPD) et d'autres des **données sensibles** au sens de l'Art. 9 RGPD : état de santé, appartenance syndicale, infractions.

Le niveau de protection requis varie selon la catégorie : les données sensibles imposent des mesures renforcées, les données ordinaires doivent simplement satisfaire aux mesures de sécurité proportionnées au risque (Art. 32 RGPD).

Conditions d’exercice

Type de données	Niveau de risque	Mesures de sécurité requises
Données ordinaires (identité, rémunération, carrière)	Risque modéré	Email professionnel avec accès contrôlé ; limitation aux destinataires habilités
Données sensibles (santé, syndicat — Art. 9 RGPD)	Risque élevé	Chiffrement de bout en bout ; plateformes RH sécurisées ; email direct entre personnes habilitées uniquement
Documents complets (bulletins de paie, dossiers médicaux)	Risque élevé	Téléchargement sécurisé sur portail RH ; envoi chiffré — email standard inadapté

Modalités pratiques

Mesure	Application
Chiffrement	Obligatoire pour données sensibles — recommandé pour toutes les données sociales
Accès limité	Pièces jointes accessibles uniquement aux destinataires habilités — éviter les groupes de diffusion larges
Traçabilité	Journalisation des envois comportant des données personnelles
Portail RH sécurisé	Solution préférable à l'email pour les documents de paie et les dossiers personnels
Procédure de violation	Documentation immédiate de toute transmission non conforme ; notification CNPD dans les **72 heures** si risque pour les personnes (Art. 33 RGPD)

Pratiques et recommandations

Établir une politique interne claire sur la transmission des données sociales, distinguant les données ordinaires (email professionnel acceptable avec mesures d'accès) des données sensibles (chiffrement obligatoire). Cette politique doit être intégrée dans le registre des traitements (Art. 30 RGPD).

Former les collaborateurs aux bonnes pratiques : ne jamais transmettre de données de santé ou d'appartenance syndicale par email standard ; utiliser les portails RH pour les documents de paie ; ne jamais inclure des données personnelles dans des destinataires Cc/Cci non habilités.

Mettre en place une procédure d'incident pour les violations de données : tout envoi erroné à un destinataire non autorisé doit être documenté et évalué selon son niveau de risque. Si le risque est élevé, notification obligatoire à la CNPD (72h) et aux personnes concernées si nécessaire.

Cadre juridique

Référence	Objet
Art. 32 RGPD (Règlement UE 2016/679)	Sécurité du traitement — mesures techniques et organisationnelles proportionnées au risque
Art. 33 RGPD	Notification des violations de données à la CNPD (72 heures)
Art. 34 RGPD	Communication aux personnes concernées en cas de risque élevé
Art. 5 RGPD	Principes : intégrité, confidentialité et sécurité des données
Art. 9 RGPD	Catégories spéciales de données — mesures renforcées (santé, syndicat, etc.)
Art. 83 RGPD	Sanctions CNPD : jusqu'à 20 M€ ou 4 % du CA mondial
Loi du 1er août 2018 (Luxembourg)	Transposition du RGPD — organisation de la CNPD

Le RGPD n'interdit pas explicitement l'email "non sécurisé" pour toutes les données sociales — il impose des mesures **proportionnées au risque**. L'absence de mesures appropriées pour des données sensibles (santé, syndicat) constitue une violation de l'Art. 32 RGPD, exposant l'employeur aux sanctions de l'Art. 83 RGPD. La CNPD peut infliger des amendes allant jusqu'à **20 millions d'euros ou 4 % du chiffre d'affaires mondial**.