Le chiffrement des données RH stockées localement est-il obligatoire ?

Réponse courte

Le **RGPD ne rend pas le chiffrement explicitement obligatoire**, mais l'article **32** impose à l'employeur des **mesures techniques appropriées** au risque. Le chiffrement est cité comme **exemple de mesure** et devient en pratique **quasi-obligatoire** dès lors que l'on traite des données sensibles ou volumineuses comme des données RH, paie ou santé.

En l'absence de chiffrement, l'employeur doit pouvoir **démontrer** que d'autres mesures offrent un niveau de sécurité équivalent. La **CNPD** considère qu'un défaut de chiffrement sur un poste portable ou un serveur local constitue un **manquement à l'obligation de sécurité** et peut alourdir significativement la sanction en cas de violation de données, notamment en cas de vol ou de perte du matériel.

Définition

Le **chiffrement** est une technique cryptographique transformant des données lisibles en données illisibles sans la clé de déchiffrement. Appliqué aux données RH stockées localement, il concerne aussi bien les **disques durs** des postes de travail que les **bases de données internes**, les **supports amovibles** et les **sauvegardes**. Il s'oppose au stockage « en clair » qui laisse les fichiers directement accessibles à toute personne disposant d'un accès physique ou logique.

Questions fréquentes

Comment gérer les clés de chiffrement RH ?

Une procédure de sauvegarde et de récupération des clés doit être documentée et testée régulièrement, pour éviter toute perte définitive de données en cas d'incident technique ou de départ d'un administrateur. La politique doit figurer au registre.

Faut-il chiffrer les sauvegardes externes ?

Oui, les sauvegardes externes et les archives doivent être sécurisées par un chiffrement distinct de celui des postes de travail, avec une gestion rigoureuse des clés. Cette mesure protège contre les vols et pertes de supports physiques.

Le chiffrement des données RH stockées localement est-il obligatoire ?

Le RGPD ne rend pas le chiffrement explicitement obligatoire, mais l'article 32 impose des mesures techniques appropriées au risque. Le chiffrement est cité comme exemple et devient en pratique quasi-obligatoire pour les données sensibles ou volumineuses.

Le chiffrement protège-t-il l'employeur en cas de violation ?

Oui, l'article 34 du RGPD prévoit qu'en cas de violation portant sur des données chiffrées devenues inexploitables, l'employeur peut être dispensé d'informer individuellement les salariés. Le chiffrement joue un rôle préventif et atténuateur.

Quelles solutions de chiffrement utiliser pour les postes RH ?

Les solutions disponibles à coût raisonnable incluent BitLocker (Windows), FileVault (macOS) et LUKS (Linux). Ces outils relèvent de l'état de l'art et permettent un chiffrement intégral du disque, conformément à l'article 32 du RGPD.

Quels supports RH doivent être chiffrés en priorité ?

Le chiffrement intégral doit être activé sur tous les postes utilisés par le service RH, la paie et la direction, y compris les ordinateurs portables et tablettes professionnelles. Les supports amovibles contenant des données RH doivent aussi être chiffrés.

Conditions d’exercice

L'article 32 RGPD impose une appréciation selon la nature des données (santé, paie), le volume, le type de support (portables, clés USB, serveurs), l'accès physique et l'état de l'art (BitLocker, FileVault, LUKS).

Critère	Détail
Nature des données	Données sensibles (santé, syndicats), données de paie, données contractuelles
Volume	Un fort volume accroît le risque et l'exigence de sécurité
Support	Portables, clés USB, serveurs internes, sauvegardes externes
Accès physique	Si plusieurs personnes ont un accès physique, le chiffrement est impératif
Finalité	Traitements RH courants relèvent d'un risque moyen à élevé
État de l'art	Solutions disponibles à coût raisonnable (BitLocker, FileVault, LUKS)

Modalités pratiques

Le déploiement du chiffrement commence par un inventaire des supports contenant des données RH, se poursuit par une analyse de risque, puis par le choix d'une solution de chiffrement et une procédure de gestion des clés documentée au registre.

Étape	Détail
Inventaire	Recensement des supports contenant des données RH
Analyse de risque	Évaluation du risque par support et par type de données
Choix de la solution	Chiffrement intégral du disque ou chiffrement par fichier
Gestion des clés	Procédure de sauvegarde et de récupération des clés
Formation	Sensibilisation du personnel RH et IT
Documentation	Inscription de la mesure au registre des traitements

Pratiques et recommandations

Activer le chiffrement intégral de disque sur tous les postes utilisés par le service RH, la paie et la direction, y compris sur les ordinateurs portables et les tablettes professionnelles.

Chiffrer systématiquement les supports amovibles contenant des données RH, en interdisant l'usage de clés USB personnelles non chiffrées pour ce type de fichiers.

Sécuriser les sauvegardes externes et les archives par un chiffrement distinct de celui des postes de travail, avec une gestion rigoureuse des clés.

Documenter la politique de chiffrement dans la charte informatique et le registre des traitements pour pouvoir démontrer la conformité à la CNPD.

Tester régulièrement la procédure de récupération des clés afin d'éviter toute perte définitive de données en cas d'incident technique ou de départ d'un administrateur.

Cadre juridique

Le chiffrement s'inscrit dans l'obligation générale de sécurité du RGPD.

Référence	Objet
Art. 32 RGPD	Mesures techniques appropriées, chiffrement cité comme exemple
Art. 5.1.f RGPD	Principe d'intégrité et de confidentialité
Art. 25 RGPD	Protection des données dès la conception et par défaut
Art. 34 RGPD	Exemption d'information en cas de données chiffrées inexploitables
Loi du 1er août 2018	Régime national et pouvoirs de la CNPD
Art. L.261-1 Code du travail	Cadre de la surveillance des salariés

L'article 34 du RGPD prévoit qu'en cas de violation portant sur des données chiffrées devenues inexploitables, l'employeur peut être dispensé d'informer individuellement les salariés. Le chiffrement joue donc à la fois un rôle préventif et un rôle d'atténuation des obligations en cas d'incident.