Comment gérer les accès aux données personnelles dans le service RH ?

Réponse courte

La gestion des accès aux données personnelles du service RH repose sur les principes de **minimisation** et de **besoin d'en connaître** issus de l'article **5 du RGPD**. Chaque utilisateur ne doit disposer que des **droits strictement nécessaires** à l'accomplissement de ses missions, dans le cadre d'une **matrice d'habilitations** formalisée et régulièrement mise à jour.

L'employeur doit mettre en place une **authentification individuelle**, une **traçabilité des consultations**, des **procédures d'attribution et de révocation** des droits, et une **revue périodique** des habilitations. En pratique, seules les personnes affectées à la paie, à l'administration du personnel ou au DPO accèdent aux données sensibles, tandis que les managers voient uniquement les informations nécessaires à leur équipe.

Définition

La **gestion des accès** recouvre l'ensemble des procédures organisationnelles et techniques définissant qui peut consulter, modifier ou supprimer des données personnelles, dans quelles conditions et pour quelle finalité. Dans un service RH, elle s'applique aux dossiers du personnel, aux bulletins de paie, aux évaluations, aux certificats médicaux et aux données disciplinaires. Elle constitue l'un des piliers de la sécurité organisationnelle exigée par le RGPD et contribue à la démonstration de conformité (accountability).

Questions fréquentes

Comment gérer les accès aux données du service RH ?

La gestion repose sur les principes de minimisation et de besoin d'en connaître issus de l'article 5 du RGPD. Chaque utilisateur doit disposer uniquement des droits strictement nécessaires à ses missions, dans le cadre d'une matrice d'habilitations formalisée.

Faut-il auditer régulièrement les accès aux données RH ?

Oui, une revue périodique des droits doit être organisée au minimum une fois par an et à chaque changement d'organisation, pour éviter les accumulations indues. L'audit est mené par le DPO et le responsable RH conjointement.

Faut-il une authentification individuelle pour les accès RH ?

Oui, l'employeur doit imposer une authentification nominative et interdire les comptes génériques ou partagés au sein du service RH. Cette mesure garantit la traçabilité individuelle des consultations et modifications, conformément à l'article 32 du RGPD.

Que doit contenir une matrice d'habilitations RH ?

La matrice formalise un tableau rôles/données avec des niveaux de droits (lecture, modification, suppression). Elle est validée conjointement avec le DPO et rattachée à la documentation du registre des traitements pour démontrer la conformité.

Quelles données RH nécessitent une journalisation des accès ?

Les accès aux données sensibles (santé, disciplinaire, rémunération) doivent être journalisés. Les journaux sont conservés suffisamment longtemps pour permettre des contrôles a posteriori, conformément à l'obligation de sécurité de l'article 32 du RGPD.

Quels risques en cas de consultation illégitime par un RH ?

Une consultation illégitime peut constituer une faute grave justifiant un licenciement et, dans certains cas, une infraction pénale. La CNPD sanctionne régulièrement les entreprises ne pouvant démontrer une gestion rigoureuse des habilitations.

Conditions d'exercice

Les articles 5.1.c (minimisation), 29 et 32 RGPD imposent un accès fondé sur le besoin d'en connaître, une authentification nominative sans compte partagé, une séparation des rôles et une revue annuelle des habilitations.

Condition	Détail
Besoin d'en connaître	L'accès est lié à la mission réelle du collaborateur
Minimisation	Seules les données nécessaires sont visibles
Authentification	Identifiant nominatif, pas de comptes partagés
Séparation des rôles	Distinction entre lecture, modification et suppression
Traçabilité	Journalisation des consultations sensibles
Revue	Contrôle annuel des habilitations

Modalités pratiques

La gestion des accès s'appuie sur une matrice rôles/données, un paramétrage automatique à l'arrivée, une révocation immédiate au départ et un audit annuel par le DPO.

Étape	Détail
Cartographie	Recensement des données et des besoins par poste
Matrice d'accès	Tableau rôles / données avec niveaux de droits
Paramétrage	Configuration dans le SIRH et les outils bureautiques
Procédure d'entrée	Attribution automatisée à l'arrivée du collaborateur
Procédure de sortie	Révocation immédiate au départ ou au changement de poste
Audit annuel	Revue des accès par le DPO et le responsable RH

Pratiques et recommandations

Formaliser une matrice d'habilitations par profil métier et la valider conjointement avec le DPO, en la rattachant à la documentation du registre des traitements.

Interdire les comptes génériques ou partagés au sein du service RH, afin de garantir une traçabilité individuelle des consultations et des modifications.

Journaliser les accès aux données sensibles (santé, disciplinaire, rémunération) et conserver les journaux suffisamment longtemps pour permettre des contrôles a posteriori.

Organiser une revue périodique des droits d'accès au minimum une fois par an et à chaque changement d'organisation, pour éviter les accumulations indues.

Former les collaborateurs RH au devoir de discrétion et aux règles internes, en leur rappelant les sanctions disciplinaires et pénales encourues en cas de consultation illégitime.

Cadre juridique

Le cadre juridique combine RGPD et obligations nationales.

Référence	Objet
Art. 5.1.c RGPD	Principe de minimisation
Art. 5.1.f RGPD	Intégrité et confidentialité
Art. 24 RGPD	Responsabilité du responsable de traitement
Art. 29 RGPD	Instructions du responsable aux personnes agissant sous son autorité
Art. 32 RGPD	Mesures de sécurité appropriées
Loi du 1er août 2018	Régime national, CNPD
Art. L.261-1 Code du travail	Surveillance des salariés et information préalable

Une consultation illégitime de dossiers par un collaborateur RH peut constituer une faute grave justifiant un licenciement et, dans certains cas, une infraction pénale. La CNPD sanctionne régulièrement les entreprises ne pouvant démontrer une gestion rigoureuse des habilitations.