

Comment maîtriser les accès aux documents RH dans une solution en ligne ?

Réponse courte

Par les habilitations et par les traces, seules mesures que le droit exige réellement. L'article **32 du RGPD** impose des mesures adaptées au risque : pour un outil hébergé, cela signifie des accès attribués par fonction, révisés aux mouvements de personnel, et une journalisation permettant de savoir qui a consulté quoi.

Trois points échappent souvent au paramétrage initial. Les **comptes d'administration**, dont les droits dépassent toujours ce que la fonction exige. Les **accès du prestataire**, qui existent pour la maintenance et doivent être encadrés par le contrat de l'article 28. Et les **comptes résiduels** des personnes ayant changé de fonction, que personne ne retire.

S'y ajoute une exigence propre à ces solutions : savoir **où** sont les données et **depuis où** elles sont accessibles, un support technique assuré depuis un pays tiers constituant un transfert.

Définition

L'**habilitation** est le droit d'accès attaché à une fonction, non à une personne. Elle se révisé lorsque la fonction change, ce que peu d'organisations font systématiquement.

La **journalisation** enregistre les consultations et les modifications. Aucun texte ne l'impose en tant que telle : elle constitue la mesure la plus simple pour démontrer que les accès étaient maîtrisés.

Conditions d'exercice

Le contrat et le paramétrage se répondent : ce que l'un prévoit, l'autre doit l'appliquer.

Point	Exigence	Base
Habilitations par fonction	Accès limité au nécessaire	RGPD, articles 5 et 32
Données sensibles	Cloisonnement des certificats médicaux	RGPD, article 9
Journalisation	Traces d'accès sur les catégories sensibles	RGPD, article 32
Accès du prestataire	Encadré par le contrat de sous-traitance	RGPD, article 28
Localisation et accès distants	Transferts identifiés et fondés	RGPD, chapitre V
Export et réversibilité	Restitution des données et des journaux	RGPD, article 28

Modalités pratiques

Le paramétrage se contrôle une fois par an ; c'est le rythme minimal pour éviter l'accumulation.

Geste	Marche à suivre
Matrice	Établir la correspondance entre fonctions et catégories de données
Comptes d'administration	Les limiter, les nommer, en tracer l'usage
Mouvements internes	Retirer les accès au changement de fonction, non au départ seulement
Prestataire	Encadrer et journaliser ses interventions
Revue annuelle	Contrôler la liste des comptes actifs et leurs droits
Export	Tester la restitution des données et des journaux

Pratiques et recommandations

Les comptes résiduels sont le défaut le plus répandu et le plus simple à corriger. Une personne ayant changé de fonction conserve souvent ses droits antérieurs faute de procédure de retrait : la revue annuelle est la mesure la plus rentable de toute politique de sécurité.

Les journaux ne survivent pas au contrat de service. Ils établissent parfaitement les accès pendant l'exploitation, puis disparaissent avec la plateforme : leur export périodique est ce qui permet de démontrer, des années plus tard, que les accès étaient maîtrisés.

L'accès du prestataire doit être visible. Un support technique disposant d'un accès permanent non journalisé rend impossible toute démonstration en cas d'incident, et le contrat de sous-traitance doit prévoir à la fois l'encadrement et la traçabilité de ces interventions.

Cadre juridique

Référence	Objet
RGPD, article 32	Mesures techniques et organisationnelles adaptées au risque
RGPD, article 28	Contrat de sous-traitance et encadrement des accès du prestataire
RGPD, article 5, paragraphe 1, point f)	Intégrité et confidentialité des données
RGPD, article 9	Interdiction de principe du traitement des données de santé
RGPD, chapitre V	Transferts hors Union, y compris par accès distant
RGPD, articles 33 et 34	Notification des violations de données

Le droit n'exige ni outil ni référentiel : il exige des accès limités au nécessaire et des traces exploitables. Exportez les journaux périodiquement, car ils disparaissent avec le contrat de service.

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.