# Sécuriser les données RH

QUESTION POSÉE

**Comment sécuriser les données RH et prouver la sécurité en cas de contrôle CNIL ?**

> **Pour être prêt en cas de contrôle CNIL, il faut produire des preuves datées : registre des traitements, règles d'accès, analyses de risques, contrats, durées de conservation et incidents traités. Une mesure non documentée est difficilement opposable lors d'un contrôle.**

## ACTIONS À METTRE EN PLACE

1. **Cartographier les traitements RH et tenir le registre à jour** immédiatement, puis à chaque évolution.

   Inscrire notamment : paie, dossiers du personnel, recrutement, contrôle d'accès, vidéosurveillance, géolocalisation, outils numériques et gestion des absences.

   Pour chaque traitement, documenter :

   - la finalité et la base juridique ;
   - les catégories de données et les personnes concernées ;
   - les destinataires et les sous-traitants ;
   - la durée de conservation ;
   - les mesures de protection et les personnes habilitées.

   Le registre constitue la pièce centrale de démonstration de conformité (**art. 30 RGPD**).

2. **Définir les accès et conserver la preuve des habilitations** à l'arrivée, au changement de poste et au départ.

   Limiter l'accès aux seules personnes qui en ont besoin : RH, paie, direction et managers selon leur périmètre. Conserver la matrice des habilitations, les validations d'accès et la trace de leur retrait lors du départ d'un salarié.

3. **Appliquer et prouver les durées de conservation** lors d'une revue au moins annuelle.

   Formaliser un tableau de conservation et des opérations de purge ou d'archivage séparé.

4. **Évaluer les traitements à risque avant leur mise en service**, avant tout déploiement ou toute modification importante.

   Réaliser une **analyse d'impact relative à la protection des données (AIPD)** lorsque le traitement présente un risque élevé : données sensibles, contrôle particulièrement intrusif, biométrie, surveillance systématique ou croisement étendu de données salariés.

   L'analyse doit décrire le traitement, évaluer les risques pour les personnes et établir les mesures retenues pour les réduire (**art. 130 du décret n° 2019-536**).

5. **Encadrer chaque prestataire RH par écrit** avant tout accès aux données.

   Pour le logiciel de paie, coffre-fort numérique, SIRH, recrutement ou prestataire informatique, vérifier l'existence d'un contrat de sous-traitance conforme à l'**art. 28 RGPD**.

   Il doit préciser, entre autres, l'objet et la durée du traitement, les données concernées, les instructions de la SA, les obligations de confidentialité, l'assistance en cas d'exercice de droits ou d'incident, et le sort des données à la fin de la prestation.

6. **Formaliser les règles internes et former les personnes concernées** à l'embauche, puis au moins une fois par an.

   Prévoir une charte ou une procédure RH/numérique : confidentialité, interdiction de partager les accès, règles de consultation des dossiers salariés et signalement d'erreurs ou d'incidents.

   Conserver les preuves de diffusion et de formation : listes d'émargement, attestations ou modules suivis.

7. **Mettre en place une procédure de violation de données** opérationnelle immédiatement.

   Désigner qui reçoit les alertes, qui décide des mesures urgentes et qui tient le registre des incidents. Documenter chaque incident, même lorsqu'il ne nécessite pas de notification.

8. **Constituer un dossier « contrôle CNIL » actualisé** lors d'une revue semestrielle.

   Y centraliser :

   - le registre des traitements ;
   - les AIPD et les décisions prises ;
   - la politique de conservation, les preuves de purge et d'archivage ;
   - la matrice des habilitations et les revues d'accès ;
   - les contrats de sous-traitance ;
   - les notices d'information salariés et candidats ;
   - les procédures d'incident et le registre des violations ;
   - les preuves de formation et les contrôles internes.

## CONSERVATION DES ACCÈS

| Donnée | Durée de conservation |
|---|---|
| Données d'identification liées au contrôle d'accès | Pendant l'habilitation, puis **6 mois** après retrait des habilitations ou cessation des fonctions |
| Journaux d'accès | En principe **3 mois** |
| Journaux d'accès utilisés de manière justifiée pour le suivi du temps de travail | **5 ans** |

Référentiel CNIL « Durées de conservation – Gestion des ressources humaines », mis à jour le 20 mai 2026.

## CONSERVATION DES DONNÉES RH

| Donnée | Conservation à prévoir |
|---|---|
| Éléments d'identification du salarié | Pendant le contrat, puis **6 ans** en archivage intermédiaire dans les conditions applicables |
| Bulletins de paie détenus par l'employeur | **5 ans** après transmission |
| Éléments de calcul des cotisations | **6 ans** |
| Images de vidéosurveillance | **1 mois maximum**, sauf extraction pour une procédure |
| Données de géolocalisation pour optimiser les tournées | **2 mois** en base active, puis **1 an** en archivage selon le référentiel |

L'archivage intermédiaire doit être séparé de la base active et accessible seulement à des personnes spécialement habilitées. Une conservation prolongée est admise lorsqu'elle répond à une obligation légale ou à un contentieux identifié, avec accès restreint.

## NOTIFICATION DES VIOLATIONS

| Situation | Action | Délai |
|---|---|---|
| Violation de données présentant un risque pour les personnes | Notifier la CNIL | Dans les **72 heures** suivant la connaissance de la violation (**art. 33 RGPD**) |
| Violation de données présentant un risque élevé | Informer aussi les personnes concernées, sauf exception légale | |
| Risque élevé subsistant malgré les mesures prises dans le cadre d'une AIPD | Consulter préalablement la CNIL | La CNIL dispose de **8 semaines**, prolongeables de **6 semaines**, pour répondre |

### À SURVEILLER

Le risque principal est l'incapacité à démontrer la conformité, même si des mesures existent en pratique. La CNIL peut demander les documents, prononcer une mise en demeure ou une sanction.

Aucun accord interne applicable n'est identifié ici. La conformité relève donc des règles RGPD et des obligations légales générales.

## RÉFÉRENCES JURIDIQUES

- **Décret, art. 130**
  Analyse d'impact à réaliser
- **Loi, art. 30**
  Registre des activités de traitement