Hébergement cloud des données RH : que dit le RGPD au Luxembourg ?

Réponse courte

Le RGPD (Règlement UE 2016/679) impose des **garanties strictes** lorsque l'employeur confie les données de ses salariés à un prestataire externe.

L'employeur reste le **responsable du traitement** au sens de l'article 4 du RGPD, même si les données sont stockées sur les serveurs d'un tiers. Il doit conclure un **contrat de sous-traitance** conforme à l'article 28, vérifier que le prestataire offre des garanties suffisantes de sécurité et s'assurer que les données restent dans l'**Espace économique européen** ou bénéficient de garanties équivalentes.

Au Luxembourg, la **CNPD** (Commission nationale pour la protection des données) est l'autorité de contrôle compétente. Elle recommandé aux employeurs de réaliser une **analyse d'impact** (AIPD) lorsque le traitement cloud porte sur des données sensibles ou concerné un grand nombre de salariés.

En cas de violation de données, le prestataire cloud doit **notifier l'employeur sans délai** et l'employeur doit notifier la CNPD dans les **72 heures** (art. 33 RGPD). Le non-respect de ces obligations expose l'employeur à des amendes pouvant atteindre **20 millions d'euros** ou **4 % du chiffre d'affaires annuel mondial**.

Définition

L'**hébergement cloud des données RH** consiste à stocker les informations relatives aux salariés (données personnelles, paie, temps de travail, évaluations) sur des serveurs gérés par un prestataire externe accessible via internet.

Le **responsable du traitement** est l'employeur qui détermine les finalités et les moyens du traitement. Le **sous-traitant** est le prestataire cloud qui traite les données pour le compte de l'employeur. La **CNPD** est l'autorité luxembourgeoise de protection des données, chargée de contrôler le respect du RGPD sur le territoire.

La distinction entre responsable du traitement et sous-traitant est fondamentale : l'employeur ne peut pas se décharger de sa responsabilité en invoquant le recours à un prestataire cloud. Il doit démontrer qu'il à choisi un sous-traitant présentant des **garanties suffisantes** (article 28 § 1 du RGPD) et qu'il à mis en place les mesures nécessaires pour assurer la conformité du traitement.

Questions fréquentes

Comment gérer les transferts hors UE ?

Privilégier un hébergement dans l'EEE ou pays avec décision d'adéquation. Pour les transferts hors EEE sans adéquation, mettre en place des clauses contractuelles types conformes au RGPD. Les transferts vers les États-Unis nécessitent une attention particulière depuis l'invalidation du Privacy Shield et son remplacement par le DPF.

Comment vérifier la sécurité du prestataire cloud ?

Vérifier le chiffrement des données en transit (TLS 1.2 minimum) et au repos (AES-256 ou équivalent). Tester les contrôles d'accès et la séparation des données entre locataires (multi-tenant). Examiner les références dans le secteur RH, exiger les rapports d'audit annuels et les certifications de sécurité (ISO 27001).

Faut-il informer les salariés du recours au cloud ?

Oui, adapter la politique de confidentialité pour mentionner le recours au cloud, l'identité du prestataire, la localisation des serveurs et les mesures de protection. Informer individuellement les salariés conformément aux articles 13 et 14 du RGPD. Mettre à jour le registre des activités de traitement (article 30).

Que doit contenir le contrat de sous-traitance ?

Le contrat conforme à l'article 28 doit inclure : objet et durée du traitement, nature et finalité, type de données et catégories de personnes, obligations du responsable, mesures de sécurité techniques et organisationnelles, conditions de recours à des sous-traitants ultérieurs, modalités de restitution, obligations de notification.

Quel délai pour notifier une violation de données ?

L'article 33 du RGPD impose à l'employeur de notifier la CNPD dans les 72 heures en cas de violation. Le prestataire cloud doit notifier l'employeur sans délai. Inclure dans le contrat une clause de notification avec un délai inférieur à 24 heures, pour laisser à l'employeur le temps de notifier la CNPD.

Quelles obligations RGPD pour l'hébergement cloud RH ?

L'employeur reste responsable du traitement même si les données sont chez un tiers. Il doit conclure un contrat de sous-traitance article 28, vérifier que le prestataire offre des garanties suffisantes de sécurité, s'assurer que les données restent dans l'EEE ou bénéficient de garanties équivalentes.

Quelles sanctions en cas de non-conformité ?

Le non-respect des obligations RGPD expose l'employeur à des amendes pouvant atteindre 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial. La CNPD peut contrôler tant l'employeur que le prestataire cloud. L'employeur ne peut transférer sa responsabilité au prestataire en invoquant le recours au cloud.

Conditions d’exercice

L'hébergement cloud des données RH est soumis à plusieurs obligations cumulatives.

Obligation	Détail
Contrat de sous-traitance	Obligatoire entre l'employeur et le prestataire cloud (art. 28 RGPD)
Localisation des données	Serveurs dans l'EEE ou pays avec décision d'adéquation ; sinon clauses contractuelles types
Mesures de sécurité	Le prestataire doit garantir confidentialité, intégrité et disponibilité (art. 32 RGPD)
Analyse d'impact (AIPD)	Recommandée si traitement à grande échelle ou données sensibles (art. 35 RGPD)
Information des salariés	Obligation d'informer sur le traitement et le sous-traitant (art. 13-14 RGPD)
Notification de violation	72 heures pour notifier la CNPD en cas de fuite de données (art. 33 RGPD)
Registre des traitements	Mentionner le sous-traitant cloud dans le registre (art. 30 RGPD)
Droit d'audit	L'employeur doit pouvoir auditer le prestataire cloud (art. 28 § 3 h RGPD)

Modalités pratiques

La mise en conformité d'un hébergement cloud RH suit des étapes précises et documentées.

1. Cartographie des données hébergées

Identifier exhaustivement toutes les données RH stockées dans le cloud : données d'identification (nom, prénom, matricule), données de paie (salaire, cotisations, retenues fiscales), données de temps de travail (horaires, absences), documents contractuels (contrat, avenants), évaluations de performance et données de formation.

Classifier ces données selon leur sensibilité pour adapter les mesures de protection. Les données de santé (certificats médicaux, avis d'aptitude) nécessitent des garanties renforcées.

2. Sélection et évaluation du prestataire cloud

Analyser la localisation exacte des centres de données et s'assurer qu'ils sont situés dans l'EEE. Examiner les références du prestataire dans le secteur RH et sa capacité à traiter des données soumises au droit luxembourgeois. Exiger la transmission des rapports d'audit annuels.

3. Rédaction du contrat de sous-traitance

Rédiger ou valider un contrat conforme à l'article 28 du RGPD, incluant au minimum : l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données et les catégories de personnes concernées, les obligations et droits du responsable du traitement, les mesures de sécurité techniques et organisationnelles, les conditions de recours à des sous-traitants ultérieurs, les modalités de restitution ou suppression des données en fin de contrat et les obligations de notification en cas de violation.

4. Réalisation de l'analyse d'impact (AIPD)

Conduire une AIPD si les critères de l'article 35 du RGPD sont remplis : traitement à grande échelle de données personnelles, utilisation de nouvelles technologies, profilage ou prise de décision automatisée.

L'AIPD doit décrire les opérations de traitement, évaluer la nécessité et la proportionnalité, identifier les risques pour les droits et libertés des salariés et définir les mesures d'atténuation.

5. Mise à jour de l'information des salariés

Adapter la politique de confidentialité interne pour mentionner le recours au cloud, l'identité du prestataire, la localisation des serveurs et les mesures de protection. Informer individuellement les salariés conformément aux articles 13 et 14 du RGPD. Mettre à jour le registre des activités de traitement (article 30 du RGPD).

6. Tests de sécurité et plan d'incident

Vérifier le chiffrement des données en transit (TLS 1.2 minimum) et au repos (AES-256 ou équivalent). Tester les contrôles d'accès et la séparation des données entre locataires (multi-tenant). Définir un plan de gestion des incidents prévoyant la notification du prestataire à l'employeur en moins de 24 heures et la notification de l'employeur à la CNPD dans les 72 heures.

7. Mise en place du plan de réversibilité

Prévoir contractuellement la récupération complète des données dans un format exploitable (CSV, XML, PDF) en cas de fin de contrat, de changement de prestataire ou de cessation d'activité du prestataire. Tester la procédure de réversibilité avant la mise en production et la renouveler périodiquement.

Pratiques et recommandations

Privilégier un prestataire cloud dont les serveurs sont situés dans l'UE où l'EEE, car tout transfert hors de cet espace nécessite des garanties supplémentaires complexes à mettre en oeuvre. Ce critère est déterminant dans le choix entre cloud et on-premise.

Inclure dans le contrat de sous-traitance une clause de notification de violation avec un délai inférieur à 24 heures, pour laisser à l'employeur le temps de notifier la CNPD dans le délai légal de 72 heures.

Informer les salariés de manière transparente sur l'identité du prestataire cloud, la localisation des serveurs et les mesures de protection mises en place, conformément aux articles 13 et 14 du RGPD.

Prévoir une clause de réversibilité permettant de récupérer l'intégralité des données dans un format exploitable en cas de changement de prestataire ou de cessation du service.

Auditer régulièrement la conformité RGPD du logiciel RH en exerçant le droit d'audit prévu par l'article 28 § 3 h du RGPD et en vérifiant le renouvellement des certifications de sécurité.

Cadre juridique

Référence	Objet
RGPD (Règlement UE 2016/679), art. 28	Obligations du sous-traitant
RGPD, art. 30	Registre des activités de traitement
RGPD, art. 32	Sécurité du traitement
RGPD, art. 33	Notification de violation à l'autorité de contrôle
RGPD, art. 35	Analyse d'impact relative à la protection des données
RGPD, art. 44-49	Transferts de données vers des pays tiers
Loi du 1er août 2018	Organisation de la CNPD et transposition nationale du RGPD

L'employeur qui héberge des données RH en cloud ne transfère pas sa responsabilité au prestataire. Il reste le responsable du traitement et doit pouvoir démontrer à tout moment sa conformité au RGPD. La CNPD peut contrôler tant l'employeur que le prestataire cloud.