Un cloud externe est-il autorisé pour stocker les dossiers RH ?

Réponse courte

Le stockage des dossiers RH sur un cloud externe est autorisé au Luxembourg, à condition de respecter strictement les obligations légales en matière de protection des données personnelles. L'employeur doit garantir la confidentialité, la sécurité, la traçabilité des accès et la conformité du prestataire cloud, notamment par un contrat de sous-traitance adapté.

Avant tout transfert, une analyse d'impact sur la protection des données peut être requise, et la localisation des serveurs doit être vérifiée pour s'assurer du niveau de protection adéquat. Les salariés doivent être informés du traitement, et l'accès aux données doit être limité aux personnes habilitées, avec des mesures de sécurité renforcées.

Définition

Le recours à un service cloud externe pour la gestion et le stockage des dossiers RH consiste à confier à un prestataire tiers l'hébergement de documents relatifs à la gestion du personnel. Ces dossiers incluent notamment les contrats de travail, bulletins de salaire, évaluations, absences, mesures disciplinaires et toutes données personnelles des salariés.

Le cloud externe implique que les données sont stockées sur des serveurs distants, accessibles via internet, et administrés par un fournisseur distinct de l'employeur. Cette externalisation soulève des enjeux spécifiques en matière de confidentialité, de sécurité et de conformité juridique.

Conditions d'exercice

L'utilisation d'un cloud externe pour les dossiers RH est autorisée au Luxembourg, sous réserve du respect strict des obligations légales en matière de protection des données à caractère personnel. L'employeur doit garantir la confidentialité, l'intégrité, la disponibilité et la sécurité des données RH, conformément au Code du travail luxembourgeois et à la législation sur la protection des données.

Le prestataire cloud doit offrir des garanties suffisantes sur le plan technique et organisationnel. Un contrat de sous-traitance conforme doit être conclu, précisant les responsabilités de chaque partie, notamment en matière de sécurité, de confidentialité et de gestion des incidents.

L'employeur doit également veiller à l'égalité de traitement entre les salariés, à la traçabilité des accès et à l'encadrement humain des traitements automatisés, conformément aux principes généraux du droit du travail.

Modalités pratiques

Avant tout transfert de dossiers RH vers un cloud externe, l'employeur doit réaliser une analyse d'impact relative à la protection des données (AIPD) si le traitement est susceptible de présenter un risque élevé pour les droits et libertés des personnes concernées.

La localisation des serveurs doit être vérifiée : le transfert de données vers un pays tiers n'est autorisé que si ce pays assure un niveau de protection adéquat reconnu par la Commission européenne ou si des garanties appropriées (clauses contractuelles types, règles d'entreprise contraignantes) sont mises en place.

Le contrat avec le prestataire doit comporter des clauses précises sur la confidentialité, la gestion des accès, la traçabilité, la réversibilité des données et la notification des violations de sécurité. L'accès aux dossiers RH doit être limité aux seules personnes habilitées, et des mesures de chiffrement et d'authentification forte doivent être mises en œuvre.

L'employeur doit informer les salariés de la nature du traitement, des finalités, de la durée de conservation, de l'identité du sous-traitant et de leurs droits, conformément à l'obligation de transparence.

Pratiques et recommandations

Il est recommandé de choisir des prestataires cloud disposant de certifications reconnues en matière de sécurité de l'information (par exemple ISO/IEC 27001). L'employeur doit documenter l'ensemble des mesures prises pour assurer la conformité, notamment en conservant les rapports d'audit, les analyses d'impact et les contrats de sous-traitance.

Une politique interne de gestion des accès et des droits doit être formalisée et régulièrement mise à jour. Il convient de prévoir des procédures de restitution ou de destruction sécurisée des données en cas de changement de prestataire ou de cessation du contrat.

L'employeur doit également consulter le comité du personnel ou la délégation du personnel, le cas échéant, lors de la mise en place ou de la modification substantielle d'un système de gestion informatisée des dossiers RH.

Cadre juridique

- Code du travail luxembourgeois :
  - Article L.261-1 et suivants (protection de la vie privée des salariés, traitement automatisé des données)
  - Article L.414-9 (consultation de la délégation du personnel sur l'introduction de moyens de surveillance)
- Loi du 1er août 2018 relative à la protection des personnes à l'égard du traitement des données à caractère personnel
- Règlement (UE) 2016/679 (RGPD)
- Décisions et recommandations de la Commission nationale pour la protection des données (CNPD)

L’employeur doit veiller à la traçabilité des accès et à l’encadrement humain des traitements automatisés. En cas de doute sur la conformité d’un projet de stockage cloud, il est fortement conseillé de consulter la CNPD, notamment pour les transferts de données hors de l’Espace économique européen ou les traitements présentant des risques particuliers pour les droits des salariés.