Peut-on stocker les documents RH sur un cloud public ?

Réponse courte

Le stockage des documents RH sur un cloud public est possible pour un employeur luxembourgeois, à condition de respecter strictement la législation nationale sur la protection des données et les obligations de sécurité. L'employeur doit notamment s'assurer que le prestataire cloud offre un niveau de sécurité approprié, que les données sont stockées dans l'EEE (ou que des garanties adéquates existent pour les transferts hors EEE), qu'un contrat de sous-traitance conforme est en place, et que l'accès aux documents est limité aux personnes habilitées.

Avant toute externalisation, il est obligatoire de réaliser une analyse d'impact si le traitement présente un risque élevé, de vérifier les certifications du prestataire, de mettre en place des mesures techniques et organisationnelles robustes, et de prévoir des procédures de gestion des incidents. L'employeur doit également garantir la traçabilité, la possibilité de récupération des données, et informer les salariés de leurs droits.

Le recours à un cloud public n'exonère jamais l'employeur de sa responsabilité en matière de protection des données RH. Tout manquement aux obligations légales peut entraîner des sanctions administratives et pénales.

Définition

Le stockage sur un cloud public désigne l'hébergement de données sur des serveurs informatiques accessibles via Internet, opérés par un prestataire tiers, mutualisés entre plusieurs clients. Les documents RH regroupent toutes les informations relatives à la gestion du personnel, telles que contrats de travail, bulletins de paie, évaluations, dossiers disciplinaires, absences et données médicales.

Ces documents contiennent des données à caractère personnel, souvent sensibles, soumises à des exigences strictes de confidentialité, d'intégrité et de disponibilité. Leur traitement doit respecter les principes de licéité, de loyauté, de transparence et de minimisation des données.

Conditions d'exercice

L'employeur peut recourir à un cloud public pour le stockage des documents RH uniquement si les conditions suivantes sont réunies :

- Le prestataire cloud garantit un niveau de sécurité approprié au regard des risques, conformément à l'article 32 de la loi du 1er août 2018 relative à la protection des personnes à l'égard du traitement des données à caractère personnel et à l'article L.261-1 du Code du travail.
- Les données sont stockées et traitées exclusivement dans l'Espace économique européen (EEE), sauf si des garanties appropriées sont mises en place pour les transferts hors EEE, telles que les clauses contractuelles types approuvées par la Commission nationale pour la protection des données (CNPD), conformément à l'article 46 de la loi précitée.
- Un contrat de sous-traitance conforme à l'article 28 de la loi du 1er août 2018 lie l'employeur (responsable du traitement) et le prestataire cloud (sous-traitant), précisant les obligations de confidentialité, de sécurité, d'assistance et de restitution ou destruction des données.
- Les accès aux documents RH sont strictement limités aux personnes habilitées, selon le principe du besoin d'en connaître, en application de l'article L.261-1 du Code du travail.
- L'égalité de traitement et la non-discrimination doivent être garanties dans la gestion des données RH, conformément à l'article L.241-1 du Code du travail.

Modalités pratiques

Avant toute externalisation sur un cloud public, l'employeur doit :

- Réaliser une analyse d'impact relative à la protection des données (AIPD) si le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, notamment en cas de traitement de données sensibles, conformément à l'article 35 de la loi du 1er août 2018.
- Vérifier que le prestataire cloud dispose de certifications de sécurité reconnues (par exemple, ISO/IEC 27001), sans que cela ne dispense de l'obligation de contrôle effectif par l'employeur.
- Mettre en place des mesures techniques et organisationnelles pour garantir la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes, conformément à l'article 32 de la loi du 1er août 2018.
- Prévoir des procédures de gestion des incidents de sécurité, de notification à la CNPD et, le cas échéant, aux personnes concernées en cas de violation de données, conformément à l'article 33 de la loi du 1er août 2018.
- S'assurer de la possibilité de récupérer l'intégralité des documents RH en cas de changement de prestataire ou de cessation du service, et de la traçabilité des accès et opérations sur les données.
- Documenter l'ensemble des mesures prises dans le registre des activités de traitement, conformément à l'article 30 de la loi du 1er août 2018.

Pratiques et recommandations

Il est recommandé de privilégier des prestataires cloud disposant d'une infrastructure localisée au Luxembourg ou dans l'EEE, afin de limiter les risques liés aux transferts internationaux de données.

L’employeur doit procéder à des audits réguliers du prestataire, vérifier la traçabilité des accès et des opérations, et documenter toutes les mesures de sécurité et de conformité. Il convient d’informer les salariés de la nature du stockage, de leurs droits d’accès, de rectification, d’opposition et d’effacement, conformément à l’article 13 de la loi du 1er août 2018.

L’utilisation de solutions de chiffrement des données, tant au repos qu’en transit, est fortement conseillée pour renforcer la sécurité. Un encadrement humain doit être assuré pour toute décision automatisée concernant les salariés, conformément à l’article 22 de la loi du 1er août 2018.

Cadre juridique

Le stockage des documents RH sur un cloud public est encadré par :

- Loi du 1er août 2018 relative à la protection des personnes à l’égard du traitement des données à caractère personnel :
  - Article 28 (sous-traitance)
  - Article 30 (registre des activités de traitement)
  - Article 32 (sécurité du traitement)
  - Article 33 (notification des violations de données)
  - Article 35 (analyse d’impact)
  - Article 46 (transferts hors EEE)
  - Article 13 (information des personnes concernées)
  - Article 22 (décisions automatisées)
- Loi du 2 août 2002 relative à la protection des personnes à l’égard du traitement des données à caractère personnel dans le secteur de l’emploi
- Code du travail luxembourgeois :
  - Article L.261-1 (protection de la vie privée des salariés)
  - Article L.241-1 (égalité de traitement)
- Lignes directrices et décisions de la CNPD, notamment en matière de sous-traitance, de sécurité et de transfert de données hors EEE

Le recours à un cloud public ne dispense jamais l’employeur de sa responsabilité pleine et entière en matière de protection des données RH. Un manquement aux obligations de sécurité, de confidentialité ou d’information expose l’employeur à des sanctions administratives et pénales prononcées par la CNPD.