Quelles précautions l’employeur doit-il prendre pour archiver les données RH dans le cloud au Luxembourg ?

Réponse courte

L’employeur doit s’assurer que l’archivage des données RH dans le cloud respecte les principes du Code du travail luxembourgeois et de la législation sur la protection des données, notamment la licéité, la loyauté, la transparence, la minimisation, la limitation de la conservation, l’intégrité, la confidentialité et la traçabilité. Il doit choisir un prestataire cloud offrant des garanties suffisantes en matière de sécurité, de confidentialité et de conformité au droit luxembourgeois, avec une préférence pour des serveurs situés au Luxembourg ou dans l’UE, et conclure un contrat écrit conforme à l’article 28 du RGPD.

Avant toute externalisation, l’employeur doit réaliser une analyse d’impact relative à la protection des données si un risque élevé est identifié, vérifier les mesures de sécurité du prestataire (chiffrement, sauvegardes, contrôle d’accès, certifications), limiter strictement l’accès aux personnes habilitées et assurer la traçabilité des opérations. Il doit également informer les salariés sur l’archivage de leurs données, traiter leurs demandes d’accès, de rectification ou d’effacement dans les délais légaux, et documenter toutes les démarches et contrôles réalisés.

L’employeur reste responsable du respect des obligations légales, doit actualiser régulièrement les mesures de sécurité et notifier toute violation de données à la CNPD et, si nécessaire, aux personnes concernées.

Définition

L’archivage des données RH dans le cloud consiste à stocker, à long terme et sous format électronique, les informations relatives aux salariés (contrats, bulletins de paie, évaluations, dossiers disciplinaires, etc.) sur des serveurs distants accessibles via Internet. Cette méthode implique le recours à des prestataires externes spécialisés dans l’hébergement et la gestion sécurisée des données, en complément ou en remplacement des supports physiques ou locaux.

L’archivage dans le cloud vise à garantir la conservation, la disponibilité et la sécurité des données RH, tout en facilitant leur accès contrôlé par les personnes habilitées. Ce procédé doit respecter les exigences légales en matière de protection des données à caractère personnel et de confidentialité.

Conditions d’exercice

L’archivage des données RH dans le cloud est soumis au respect des principes fondamentaux du Code du travail luxembourgeois et de la législation sur la protection des données. L’employeur doit veiller à la licéité, la loyauté, la transparence, la minimisation, la limitation de la conservation, l’intégrité, la confidentialité et la traçabilité des données archivées.

Le recours à un prestataire cloud est autorisé à condition que celui-ci présente des garanties suffisantes en matière de sécurité, de confidentialité et de conformité au droit luxembourgeois. L'employeur demeure responsable du traitement, même en cas de sous-traitance, et doit s'assurer que le prestataire respecte les instructions et obligations légales.

L'égalité de traitement entre les salariés, la traçabilité des accès et l'encadrement humain des processus automatisés doivent être assurés à chaque étape de l'archivage.

Modalités pratiques

Avant toute externalisation, l'employeur doit réaliser une analyse d'impact relative à la protection des données (AIPD) si l'archivage est susceptible de présenter un risque élevé pour les droits et libertés des personnes concernées (article 35 RGPD, repris par la loi du 1er août 2018).

Le choix du prestataire cloud doit être précédé d'une vérification approfondie portant sur :

- La localisation des serveurs (préférence pour le Luxembourg ou l'UE, ou pays reconnus adéquats)
- Les mesures de sécurité techniques et organisationnelles (chiffrement, sauvegardes, contrôle d'accès)
- Les certifications pertinentes (ex. ISO/IEC 27001)
- La capacité à respecter les instructions de l'employeur en tant que responsable du traitement

Un contrat écrit, conforme à l'article 28 du RGPD et à la loi du 1er août 2018, doit être conclu avec le sous-traitant. Ce contrat doit préciser : la nature des données, la durée de conservation, les modalités de restitution ou de destruction, les obligations en cas de violation de données, et les mesures de sécurité attendues.

L'employeur doit informer les salariés de l'archivage de leurs données dans le cloud, conformément à l'obligation de transparence (article 13 RGPD et article 41 du Code du travail).

Pratiques et recommandations

Il est recommandé de privilégier des prestataires disposant de centres de données situés au Luxembourg ou, à défaut, dans des pays offrant un niveau de protection reconnu comme adéquat par la Commission européenne.

L'accès aux données doit être strictement limité aux personnes habilitées, avec une gestion rigoureuse des droits d'accès et une traçabilité complète des opérations. Des procédures de sauvegarde régulière, de chiffrement des données en transit et au repos, ainsi que des tests périodiques de restauration doivent être mis en place.

L'employeur doit actualiser régulièrement les mesures de sécurité en fonction de l'évolution des risques et des exigences légales. Il est conseillé de documenter toutes les démarches et de conserver la preuve des contrôles réalisés.

L'information des salariés sur la finalité, la durée et les modalités de l'archivage dans le cloud est obligatoire. Toute demande d'accès, de rectification ou d'effacement doit être traitée dans les délais légaux.

Cadre juridique

L’archivage des données RH dans le cloud est encadré par :

- **Code du travail luxembourgeois** :
  - Article L.261-1 et suivants (protection des données à caractère personnel dans la relation de travail)
  - Article L.121-6 (égalité de traitement)
  - Article L.414-3 (consultation du personnel sur l’introduction de nouvelles technologies)
- **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)** :
  - Article 5 (principes relatifs au traitement)
  - Article 13 (information des personnes concernées)
  - Article 28 (sous-traitance)
  - Article 32 (sécurité du traitement)
  - Article 35 (analyse d’impact)
  - Article 33 (notification des violations)
- **Jurisprudence et recommandations de la CNPD Luxembourg**

L’employeur reste responsable du respect des principes de licéité, de loyauté, de minimisation, de limitation de la conservation, de sécurité et de confidentialité. Toute violation de données doit être notifiée à la CNPD et, le cas échéant, aux personnes concernées, dans les meilleurs délais.

L’archivage des données RH dans le cloud ne dispense pas l’employeur de ses obligations légales en matière de sécurité, de confidentialité et de respect des droits des salariés. Il est impératif de vérifier régulièrement la conformité du prestataire, de documenter les contrôles et d’actualiser les mesures de sécurité selon l’évolution des risques et de la législation.