Que risque un employeur qui diffuse des données personnelles RH sur un canal non sécurisé ?

Réponse courte

Un employeur qui diffuse des données personnelles RH sur un canal non sécurisé au Luxembourg s'expose à des contrôles de la CNPD, à des injonctions de mise en conformité, à la limitation ou à l'interdiction du traitement des données, ainsi qu'à des sanctions administratives pouvant aller jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial, selon le montant le plus élevé. La responsabilité de l'employeur est engagée même en l'absence de préjudice effectif pour les personnes concernées.

En cas de violation de données à caractère personnel, l'employeur doit notifier la CNPD dans un délai maximum de 72 heures après en avoir eu connaissance, conformément à l'article 33(1) du RGPD et de la loi du 1er août 2018. Si la violation est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, l'employeur doit également informer sans délai ces personnes, conformément à l'article 34 du RGPD et de la loi du 1er août 2018.

Les salariés dont les données ont été diffusées peuvent engager la responsabilité civile de l'employeur pour obtenir réparation du préjudice subi. Toute violation doit être documentée par l'employeur, conformément à l'article 33(5) du RGPD.

Définition

La diffusion de données personnelles RH sur un canal non sécurisé désigne toute transmission, partage ou mise à disposition d'informations relatives à l'identité, la situation professionnelle, la rémunération, la santé ou tout autre élément personnel d'un salarié, par un moyen de communication qui ne garantit pas la confidentialité, l'intégrité et la sécurité des données.

Sont notamment concernés les envois par courriel non chiffré, messageries instantanées non sécurisées, plateformes de stockage non protégées ou tout support accessible à des tiers non autorisés. La protection de ces données relève d'une obligation de confidentialité prévue à l'article L.121-6 du Code du travail luxembourgeois, qui impose à l'employeur de garantir la confidentialité des informations relatives aux salariés.

Conditions d'exercice

L'employeur est tenu, en vertu de la loi modifiée du 1er août 2018 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, d'assurer la sécurité des données traitées dans le cadre de la gestion RH. La diffusion sur un canal non sécurisé constitue un manquement dès lors que les mesures techniques et organisationnelles appropriées n'ont pas été mises en œuvre pour prévenir tout accès non autorisé, altération, perte

ou divulgation illicite des données.

La responsabilité de l'employeur est engagée indépendamment de l'existence d'un dommage effectif pour la personne concernée. L'obligation de confidentialité des données des salariés, prévue à l'article L.121-6 du Code du travail, s'applique à toute manipulation ou transmission de données RH.

Modalités pratiques

En cas de diffusion non sécurisée, la Commission nationale pour la protection des données (CNPD) peut être saisie par la personne concernée ou agir d'office. L'employeur doit notifier la CNPD dans les 72 heures après avoir eu connaissance de la violation, conformément à l'article 33(1) du RGPD et de la loi du 1er août 2018.

Si la violation est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, l'employeur doit informer sans délai ces personnes, conformément à l'article 34 du RGPD et de la loi du 1er août 2018. Toute violation doit être documentée, en précisant les faits, les effets et les mesures prises, conformément à l'article 33(5) du RGPD.

L'employeur s'expose à des contrôles, à une injonction de mise en conformité, à la limitation ou à l'interdiction du traitement, ainsi qu'à des sanctions administratives. Les salariés concernés peuvent également engager la responsabilité civile de l'employeur pour obtenir réparation du préjudice subi.

Pratiques et recommandations

Il est impératif d'utiliser des canaux de communication sécurisés pour toute transmission de données RH : courriels chiffrés, plateformes internes protégées, accès restreints par authentification forte. Les procédures internes doivent prévoir la classification des données, la sensibilisation du personnel, la traçabilité des accès et la gestion des incidents de sécurité.

Toute faille ou diffusion accidentelle doit faire l'objet d'une analyse immédiate, d'une documentation détaillée et, le cas échéant, d'une notification à la CNPD dans les 72 heures et aux personnes concernées si le risque est élevé. La désignation d'un délégué à la protection des données (DPO) est obligatoire pour tout organisme public et pour les employeurs privés dont l'activité principale consiste en des traitements exigeant un suivi régulier et systématique à grande échelle, ou qui traitent à grande échelle des catégories particulières de données, conformément à l'article 37 du RGPD et de la loi du 1er août 2018.

Cadre juridique

La loi du 1er août 2018 relative à la protection des personnes à l'égard du traitement des données à caractère personnel transpose et complète les obligations en matière de sécurité des données. L'article 33 impose la notification à la CNPD dans les 72 heures en cas de violation de données à caractère personnel. L'article 34 impose l'information sans délai des personnes concernées en cas de risque élevé pour leurs droits et libertés. L'article 33(5) du RGPD impose la documentation de toute violation.

L’article L.121-6 du Code du travail luxembourgeois impose à l’employeur une obligation de confidentialité sur les données relatives aux salariés. L’article 42 de la loi du 1er août 2018 prévoit des sanctions administratives pouvant atteindre 20 millions d’euros ou 4 % du chiffre d’affaires annuel mondial, selon le montant le plus élevé. La CNPD dispose d’un pouvoir de contrôle, d’enquête et de sanction.

- Article 33, 34, 37 et 42 du RGPD et de la loi du 1er août 2018
- Article L.121-6 du Code du travail luxembourgeois

La négligence dans la sécurisation des données RH expose l’employeur à des sanctions lourdes et à une atteinte à sa réputation. Il est essentiel de documenter toutes les mesures de sécurité mises en place, de conserver une trace de chaque violation et de former régulièrement le personnel à la gestion des données personnelles.