

Le canal de signalement peut-il être hébergé en dehors de l'UE ?

Réponse courte

Le canal de signalement peut être hébergé en dehors de l'UE uniquement si le pays de destination assure un niveau de protection des données jugé adéquat par la Commission européenne. À défaut, l'employeur doit mettre en place des garanties appropriées, telles que les clauses contractuelles types, et prendre des mesures supplémentaires pour garantir un niveau de protection équivalent à celui de l'EEE.

Avant tout transfert, il est obligatoire de vérifier la décision d'adéquation, de conclure les contrats nécessaires, de réaliser une analyse d'impact si besoin, et d'informer les personnes concernées sur le transfert et leurs droits. Il est fortement recommandé de privilégier un hébergement au sein de l'EEE afin de limiter les risques juridiques et opérationnels.

Définition

Le canal de signalement est un dispositif interne permettant aux salariés, ainsi qu'aux personnes assimilées, de signaler de manière confidentielle des faits constitutifs d'infractions, de violations ou de risques graves au sein de l'entreprise. Au Luxembourg, la mise en place d'un canal de signalement interne est obligatoire pour les employeurs d'au moins 50 salariés, conformément à la loi du 16 mai 2023 relative à la protection des lanceurs d'alerte. L'hébergement du canal fait référence à l'emplacement physique ou virtuel où sont stockées et traitées les données issues des signalements, incluant les données à caractère personnel.

Conditions d'exercice

L'hébergement du canal de signalement doit respecter les principes de confidentialité, d'intégrité, de sécurité et de traçabilité des données à caractère personnel, conformément à la loi modifiée du 1er août 2018 et au Règlement (UE) 2016/679 (RGPD) tel qu'appliqué au Luxembourg. Le transfert de données à caractère personnel vers un pays tiers, c'est-à-dire hors de l'Espace économique européen (EEE), n'est autorisé que si ce pays assure un niveau de protection adéquat reconnu par une décision de la Commission européenne (article 44 et suivants du RGPD, article 65 de la loi du 1er août 2018). À défaut, des garanties appropriées doivent être mises en place, telles que les clauses contractuelles types adoptées par la Commission européenne, et des mesures supplémentaires peuvent être requises pour assurer un niveau de protection équivalent à celui garanti dans l'EEE.

Modalités pratiques

Avant tout hébergement du canal de signalement en dehors de l'UE, l'employeur doit vérifier si le pays de destination bénéficie d'une décision d'adéquation de la Commission européenne (article 45 RGPD). Si ce n'est pas le cas, il doit conclure des clauses contractuelles types (article 46 RGPD) avec le prestataire hébergeant les données et procéder

à une analyse d'impact relative à la protection des données (DPIA) si le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées (article 35 RGPD, article 63 de la loi du 1er août 2018). L'employeur doit informer les personnes concernées du transfert, de ses finalités, des garanties mises en place et des modalités d'exercice de leurs droits (articles 13 et 14 RGPD). Toute sous-traitance doit faire l'objet d'un contrat conforme à l'article 28 RGPD, précisant les instructions, les mesures de sécurité et les obligations du sous-traitant.

Pratiques et recommandations

Il est recommandé de privilégier l'hébergement du canal de signalement au Luxembourg ou dans un autre État membre de l'EEE afin de limiter les risques juridiques et opérationnels liés au transfert de données hors EEE. En cas d'hébergement dans un pays tiers, l'employeur doit documenter l'ensemble des mesures techniques et organisationnelles mises en œuvre pour garantir la confidentialité, la sécurité et la traçabilité des données. Il est conseillé de consulter le délégué à la protection des données (DPO) et, en cas de doute, de solliciter l'avis préalable de la Commission nationale pour la protection des données (CNPD). L'égalité de traitement des personnes concernées et l'encadrement humain du dispositif doivent être assurés. Toute violation des obligations en matière de transfert de données peut entraîner des sanctions administratives et pénales prévues par la législation luxembourgeoise.

Cadre juridique

- Loi du 16 mai 2023 relative à la protection des lanceurs d'alerte
- Loi modifiée du 1er août 2018 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, notamment articles 62 à 67
- Règlement (UE) 2016/679 du 27 avril 2016 (RGPD), notamment articles 13, 14, 28, 35, 44 à 50
- Décisions et recommandations de la Commission nationale pour la protection des données (CNPD)
- Décisions d'adéquation de la Commission européenne

L'hébergement du canal de signalement en dehors de l'EEE impose à l'employeur des obligations renforcées en matière de documentation, de sécurité et de transparence. Il est impératif de privilégier, autant que possible, un hébergement au sein de l'EEE et de documenter chaque étape du transfert, sous peine de sanctions administratives et pénales.

Les contenus sont rédigés et mis à jour régulièrement à partir de sources officielles. Leur usage ne remplace pas une consultation juridique et doit être validé par un professionnel du droit.