Une entreprise peut-elle utiliser un outil SaaS pour gérer les alertes internes ?

Réponse courte

L'utilisation d'un outil SaaS pour la gestion des alertes internes est légalement autorisée au Luxembourg, sous réserve du respect strict des obligations définies par la loi du 16 mai 2023 sur la protection des lanceurs d'alerte et le RGPD. Le système doit garantir la confidentialité des signalements et l'identité des personnes concernées, avec un hébergement des données dans l'EEE et une analyse d'impact obligatoire préalable.

Définition

Le canal d'alerte interne désigne tout dispositif permettant aux travailleurs de signaler des violations présumées au sein de leur organisation. Un outil SaaS (Software as a Service) est une solution logicielle accessible en ligne permettant de gérer de manière sécurisée la réception, le traitement et le suivi des alertes, conformément aux exigences légales de confidentialité et de traçabilité.

Conditions d’exercice

L'employeur doit respecter plusieurs conditions cumulatives :

- Réaliser une analyse d'impact relative à la protection des données (AIPD)
- Sélectionner un prestataire offrant des garanties suffisantes (art. 28 RGPD)
- Conclure un contrat de sous-traitance conforme au RGPD
- Garantir un hébergement des données dans l'EEE
- Mettre en place des mesures techniques et organisationnelles appropriées
- Assurer la formation des personnes habilitées à traiter les alertes

Modalités pratiques

La mise en place requiert :

- La désignation d'un responsable interne du dispositif d'alerte
- L'information préalable des représentants du personnel
- La documentation complète du système dans le registre des traitements
- La mise en place de procédures écrites pour le traitement des alertes
- Un système de gestion des accès strictement contrôlé
- Des mesures de sécurité adaptées (chiffrement, traçabilité)

Pratiques et recommandations

Il est recommandé de :

- Privilégier des solutions certifiées ou labellisées
- Effectuer des audits réguliers du prestataire
- Mettre en place une procédure de test régulière
- Prévoir des formations régulières des utilisateurs
- Documenter toutes les mesures de sécurité mises en œuvre
- Établir un plan de continuité en cas de défaillance du système

Cadre juridique

- Loi du 16 mai 2023 relative à la protection des lanceurs d'alerte :
  - Art. 6 : Obligation de mise en place de canaux de signalement interne
  - Art. 7 : Conditions de confidentialité et de sécurité
  - Art. 8 : Délais de traitement et suivi des signalements
- Code du travail luxembourgeois :
  - Art. L.271-1 et suivants : Protection des lanceurs d'alerte
  - Art. L.261-1 : Protection des données des salariés
- RGPD :
  - Art. 28 : Obligations relatives à la sous-traitance
  - Art. 32 : Sécurité du traitement
  - Art. 35 : Analyse d'impact relative à la protection des données

L'employeur reste juridiquement responsable du traitement des alertes même en cas d'externalisation via un outil SaaS. La CNPD peut contrôler à tout moment la conformité du dispositif et sanctionner les manquements constatés.