Quel lien entre lanceurs d’alerte et RGPD ?

Réponse courte

Le lien entre lanceurs d’alerte et RGPD réside dans le fait que tout dispositif d’alerte professionnelle implique le traitement de données à caractère personnel, telles que l’identité du lanceur d’alerte, de la personne mise en cause et de tout tiers mentionné. Ce traitement doit respecter les principes du RGPD : licéité, loyauté, transparence, minimisation, sécurité et confidentialité.

La mise en place d’un dispositif d’alerte nécessite une analyse d’impact relative à la protection des données, une information claire des personnes concernées sur leurs droits, et une limitation stricte de l’accès aux données aux seules personnes habilitées. La conservation, la suppression et la transmission des données doivent être encadrées et documentées, sous le contrôle de la CNPD et en consultation avec le DPO.

Définition

Un **lanceur d’alerte** est une personne physique qui signale ou divulgue, dans un contexte professionnel, des informations concernant des violations effectives ou potentielles du droit luxembourgeois, dont elle a eu connaissance dans le cadre de ses activités professionnelles. La protection des données à caractère personnel, encadrée par le Règlement (UE) 2016/679 (RGPD) et la loi modifiée du 1er août 2018, s’applique à tout traitement de données effectué dans le cadre d’un dispositif d’alerte professionnelle.

Les données concernées incluent l’identité du lanceur d’alerte, de la personne mise en cause, ainsi que de tout tiers mentionné dans le signalement. Le traitement de ces données doit respecter les principes de licéité, loyauté, transparence, minimisation et sécurité.

Conditions d’exercice

La mise en place d’un dispositif d’alerte interne implique la collecte et le traitement de données à caractère personnel, qui doivent être strictement limitées aux informations nécessaires à la gestion du signalement. L’accès aux données est réservé aux seules personnes habilitées à instruire l’alerte, dans le respect du principe de confidentialité.

Le responsable du traitement doit garantir la confidentialité de l’identité du lanceur d’alerte, de la personne visée et de tout tiers mentionné, sauf obligation légale contraire. Le traitement des données dans ce contexte repose sur le respect d’une obligation légale (article L.271-1 et suivants du Code du travail) ou sur l’intérêt légitime du responsable du traitement, sous réserve de l’équilibre avec les droits et libertés des personnes concernées.

L’égalité de traitement et la non-discrimination doivent être assurées à l’égard du lanceur d’alerte et des personnes visées par le signalement, conformément aux articles L.241-1 et L.251-1 du Code du travail.

Modalités pratiques

Avant la mise en place d'un dispositif d'alerte, une **analyse d'impact relative à la protection des données (AIPD)** est requise, conformément à l'article 35 du RGPD, en raison du caractère sensible des traitements. Les personnes concernées doivent être informées de l'existence du dispositif, de ses finalités, des modalités de traitement, des destinataires des données, de la durée de conservation et des droits dont elles disposent (articles 13 et 14 du RGPD).

Les données relatives à un signalement infondé ou non suivi d'effet doivent être supprimées sans délai. Les données relatives à un signalement avéré peuvent être conservées pour la durée strictement nécessaire à la gestion du dossier, sans excéder cinq ans à compter de la clôture de la procédure, sauf contentieux en cours.

L'accès aux données est strictement limité aux personnes chargées du traitement de l'alerte. La traçabilité des accès et des traitements doit être assurée, et toute transmission d'informations à des tiers, y compris aux autorités compétentes, doit être documentée.

Pratiques et recommandations

Il est recommandé de désigner un point de contact unique pour la gestion des alertes et de formaliser les procédures internes relatives à la réception, l'instruction et la conservation des signalements. Les responsables RH doivent veiller à ce que l'ensemble du personnel soit informé des droits relatifs à la protection des données, notamment le droit d'accès, de rectification, de limitation et d'effacement.

La formation des personnes habilitées à traiter les alertes sur les obligations en matière de confidentialité et de protection des données est essentielle. Il convient d'assurer la traçabilité des accès et des traitements liés aux alertes, et de consulter le délégué à la protection des données (DPO) avant toute modification substantielle du dispositif.

L'encadrement humain du dispositif doit être garanti, notamment pour éviter toute décision automatisée sans intervention humaine, conformément à l'article 22 du RGPD.

Cadre juridique

- Loi du 16 mai 2023 relative à la protection des personnes qui signalent des violations du droit national (articles 1 à 36)
- Code du travail luxembourgeois :
  - Article L.271-1 et suivants (protection des lanceurs d’alerte)
  - Article L.241-1 (égalité de traitement)
  - Article L.251-1 (non-discrimination)
- Règlement (UE) 2016/679 (RGPD) :
  - Article 5 (principes relatifs au traitement)
  - Article 6 (licéité du traitement)
  - Article 13 et 14 (information des personnes concernées)
  - Article 22 (décisions automatisées)
  - Article 32 (sécurité du traitement)
  - Article 35 (analyse d’impact)
- Loi modifiée du 1er août 2018 relative à la protection des personnes à l’égard du traitement des données à caractère personnel (articles 1 à 70)
- Contrôle de la CNPD (Commission nationale pour la protection des données)

Documentez systématiquement l’ensemble des traitements liés aux dispositifs d’alerte dans le registre des activités de traitement. Consultez le délégué à la protection des données (DPO) avant toute modification substantielle du dispositif et veillez à garantir l’encadrement humain de toute procédure automatisée.