# Comment les informations du lanceur d’alerte doivent-elles être protégées au regard du RGPD ?

## Réponse courte

Les informations du lanceur d’alerte doivent être protégées en appliquant strictement les principes du RGPD : licéité, loyauté, transparence, limitation des finalités, minimisation, exactitude, limitation de la conservation, intégrité et confidentialité. L’accès à ces données est limité aux personnes habilitées, spécifiquement désignées pour la gestion des alertes, et toute communication de l’identité du lanceur d’alerte nécessite son consentement exprès, sauf obligation légale ou décision judiciaire.

L’employeur doit mettre en place des procédures internes garantissant la confidentialité, utiliser des mesures techniques et organisationnelles appropriées (chiffrement, accès restreint, traçabilité), et informer le lanceur d’alerte sur le traitement de ses données et ses droits. Les données doivent être conservées uniquement le temps nécessaire à l’instruction de l’alerte, puis supprimées ou anonymisées. Toute violation de données doit être notifiée à la CNPD et, si besoin, aux personnes concernées.

## Définition

Le lanceur d’alerte est une personne qui signale ou divulgue, dans un contexte professionnel, des faits susceptibles de constituer une violation grave du droit luxembourgeois. Les informations relatives au lanceur d’alerte comprennent toutes les données permettant de l’identifier directement ou indirectement, ainsi que les éléments relatifs à l’alerte elle-même.

Ces données sont considérées comme des données à caractère personnel au sens du Règlement (UE) 2016/679 (RGPD) et de la loi modifiée du 1er août 2018 relative à la protection des personnes physiques à l’égard du traitement des données à caractère personnel.

## Conditions d’exercice

La collecte, le traitement et la conservation des informations du lanceur d’alerte doivent respecter les principes fondamentaux du RGPD, notamment :

- la licéité, la loyauté et la transparence du traitement,
- la limitation des finalités,
- la minimisation des données,
- l'exactitude,
- la limitation de la conservation,
- l'intégrité et la confidentialité.

Le traitement est licite s'il repose sur une obligation légale (article L.271-1 et suivants du Code du travail), l'intérêt légitime de l'employeur à prévenir ou détecter des manquements graves, ou le consentement explicite du lanceur d'alerte.

L'accès aux données doit être strictement limité aux personnes habilitées, spécifiquement désignées pour la gestion des alertes internes, conformément à l'article 38 de la loi du 16 mai 2023.

## Modalités pratiques

L'employeur doit mettre en place des procédures internes garantissant la confidentialité de l'identité du lanceur d'alerte et des tiers mentionnés dans l'alerte. Les systèmes d'alerte doivent être sécurisés, avec des mesures techniques et organisationnelles appropriées telles que le chiffrement, l'accès restreint et la traçabilité des accès.

Toute communication d'informations permettant d'identifier le lanceur d'alerte ne peut intervenir sans son consentement exprès, sauf obligation légale ou décision judiciaire (article 36 de la loi du 16 mai 2023). Les données ne doivent être conservées que le temps strictement nécessaire à l'instruction de l'alerte et à la clôture des procédures afférentes, puis supprimées ou anonymisées.

L'information du lanceur d'alerte sur le traitement de ses données, ses droits d'accès, de rectification, d'effacement et de limitation, ainsi que sur les modalités d'exercice de ces droits, est obligatoire dès la réception de l'alerte (articles 13 et 14 du RGPD).

## Pratiques et recommandations

Il est recommandé de désigner un responsable du traitement ou un délégué à la protection des données (DPO) chargé de superviser la conformité des traitements liés aux alertes. Les responsables RH doivent veiller à la formation du personnel habilité à traiter les alertes, à la documentation des procédures et à la réalisation régulière d'analyses d'impact sur la protection des données (DPIA) lorsque le traitement présente un risque élevé pour les droits et libertés des personnes concernées.

Toute violation de données doit être notifiée à la Commission nationale pour la protection des données (CNPD) dans les meilleurs délais et, si nécessaire, aux personnes concernées (articles 33 et 34 du RGPD). Les sous-traitants impliqués dans la gestion des alertes doivent faire l'objet de clauses contractuelles spécifiques garantissant le respect des obligations prévues par le RGPD et la législation luxembourgeoise.

## Cadre juridique

- Règlement (UE) 2016/679 (RGPD), notamment articles 5, 6, 9, 13, 14, 24, 25, 32, 33, 34
- Loi modifiée du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel
- Loi du 16 mai 2023 relative à la protection des personnes qui signalent des violations du droit national, notamment articles 36 à 38
- Code du travail luxembourgeois, articles L.271-1 et suivants
- Lignes directrices de la CNPD sur les dispositifs d'alerte professionnelle

La divulgation non autorisée de l'identité du lanceur d'alerte ou la conservation excessive de ses données expose l'employeur à des sanctions administratives et pénales prononcées par la CNPD et les juridictions luxembourgeoises. Il est essentiel d'assurer la traçabilité des accès et de garantir l'encadrement humain du dispositif d'alerte.