



POLITIQUE AUX LANCEURS D'ALERTE





TABLEAU DES CONTENUS

À qui s'applique cette politique ?	3
Que faut-il signaler ?	4
Comment faire un rapport ?	5
Comment et par qui sont traités les rapports ?	7
Comment protéger les lanceurs d'alerte contre les représailles ?	10
Combien de temps se gardent les rapports ?	14

À QUI S'APPLIQUE CETTE POLITIQUE ?

Cette politique s'applique aux lanceurs d'alerte. Un lanceur d'alerte est toute personne qui adresse un signal d'alarme en espérant enclencher un processus de régulation ou de mobilisation collective, après avoir eu connaissance d'un risque dans un contexte lié au travail.

Il s'agit notamment d'employés actuels ou d'anciens employés, des travailleurs indépendants, d'actionnaires et de personnes appartenant à l'organe de direction ou de surveillance de l'entreprise, y compris leurs membres non cadres, ainsi que de bénévoles, stagiaires rémunérés ou pas, de clients et de toute personne travaillant sous la supervision et la direction d'associés, d'entrepreneurs, sous-traitants et fournisseurs.

La présente politique s'applique également aux lanceurs d'alerte dont la relation de travail n'a pas encore commencé, dans les cas où des informations sur des infractions ont été obtenues au cours du processus de recrutement ou d'autres négociations précontractuelles.

La protection prévue par la présente politique est également accordée aux personnes (facilitateurs) qui aident les lanceurs d'alerte dans le processus de signalement, aux tiers qui sont liés aux lanceurs d'alerte (collègues ou famille) et qui pourraient subir des représailles dans un contexte professionnel, ainsi qu'aux entités juridiques que le lanceur d'alerte possède, pour lesquelles il travaille ou avec lesquelles il est lié d'une autre manière dans un contexte professionnel.

QUE FAUT-IL SIGNALER ?

Le canal de signalement interne est destiné aux rapports dans lesquels un lanceur d'alerte a au moins des soupçons raisonnables concernant des infractions réelles ou potentielles qui se sont produites, qui sont actuellement en cours ou qui sont susceptibles de se produire, ainsi que des tentatives de dissimulation de ces infractions.

Une infraction est un acte ou une omission qui est illégal et qui concerne notre entreprise, ou qui va à l'encontre de l'objet ou du but de la législation, de nos politiques et/ou de nos règlements internes. Une infraction peut inclure, sans s'y limiter, les éléments suivants :

- les pots-de-vin ou la corruption
- la fraude, le blanchiment de capitaux, le vol ou l'utilisation inappropriée des biens ou des fonds de l'entreprise,
- les conflits d'intérêts non déclarés ou mal gérés,
- les pratiques anticoncurrentielles,
- le délit d'initié ou l'abus de marché,
- la violation de sanctions,
- les irrégularités financières,
- la violation de la confidentialité des données,
- la négligence grave, l'intimidation, la discrimination illicite, le harcèlement sur le lieu de travail ou le harcèlement sexuel,
- le gaspillage ou la mauvaise gestion,
- les pratiques de travail dangereuses et autres problèmes importants de sécurité ou de santé,
- l'esclavage moderne et la ou les violations des droits de l'homme,
- les préjudices importants à l'environnement,
- les représailles contre le lanceur d'alerte ou contre toute autre personne protégée en vertu de la présente politique,
- tout comportement contraire aux principes moraux, aux règles ou aux normes de l'entreprise, ou à la loi.

COMMENT FAIRE UN RAPPORT ?

Le personnel autorisé (voir ci-dessous) est disponible pour vous soutenir et vous conseiller lors du processus de lancement d'alerte en entreprise.

CANAUX DE SIGNALEMENT

Les rapports peuvent être soumis en utilisant le canal de signalement en ligne de l'entreprise Trusty (lien ici).

En outre, les rapports peuvent être soumis par le biais d'autres canaux, énumérés sur la plateforme Trusty ou dans un document séparé. Lorsque le lanceur d'alerte soumet le rapport par le biais de ces canaux, il est incité à fournir les coordonnées où il souhaite recevoir l'accusé de réception du rapport, ainsi que les commentaires sur le rapport de l'entreprise.

Vous pouvez toujours solliciter un rendez-vous physique avec le personnel autorisé et lui soumettre votre rapport directement.

Les lanceurs d'alerte sont également libres d'effectuer des signalements à l'extérieur de l'entreprise. Ces rapports doivent être adressés à l'autorité compétente, comme indiqué dans un document distinct.



CONTENU DU RAPPORT **ET IDENTITÉ DU LANCEUR D'ALERTE**

Le rapport doit contenir autant de détails que possible sur qui, quoi, où, quand, comment et pourquoi sur l'infraction signalée, ainsi que toute preuve à l'appui. Toute information complémentaire sur la manière dont l'entreprise pourrait traiter au mieux l'infraction signalée est souhaitable.

Les lanceurs d'alerte peuvent soumettre des rapports de manière anonyme ou choisir de divulguer leur identité.

La plateforme Trusty vous permet une communication anonyme bidirectionnelle, même si un lanceur d'alerte choisit de signaler une violation sans divulguer son identité.

Les lanceurs d'alerte sont encouragés à s'identifier. Cela permet un traitement plus productif et plus efficace de leurs rapports et les protège en cas de représailles.

L'identité des lanceurs d'alerte, ainsi que toute autre information permettant de déduire directement ou indirectement leur identité, n'est divulguée à personne, en dehors du personnel autorisé compétent pour recevoir et suivre les rapports, sans le consentement explicite du lanceur d'alerte. Nonobstant, l'entreprise donne l'identité d'un lanceur d'alerte lorsque la loi le lui exige, en informant le lanceur d'alerte avant de le faire ; sauf si cette information risque de compromettre les enquêtes ou les procédures judiciaires qui s'y rapportent.

Toute tentative non autorisée d'identification d'un lanceur d'alerte ou d'une personne concernée est interdite et fera l'objet de sanctions disciplinaires.

COMMENT ET PAR QUI SONT TRAITÉS LES RAPPORTS ?

PERSONNEL AUTORISÉ

Le canal de signalement interne de l'entreprise est géré par le personnel autorisé et désigné dans un document distinct. Ce personnel est chargé de recevoir les rapports et d'en assurer le suivi.

Le personnel autorisé dispose d'un accès direct, illimité et confidentiel à l'organe directeur et à la direction générale de l'entreprise, auxquels il rend les comptes sur la gestion du système d'alertes. Le personnel autorisé dispose d'un accès direct, sans restriction aux ressources nécessaires pour garantir l'impartialité, l'intégrité et la transparence du système de gestion des alertes et de ses processus.

TRAITEMENT DES RAPPORTS

Le traitement d'une déclaration se déroule comme suit, en fonction du contenu de la déclaration et de sa nature :

- **Reçu** : l'entreprise reçoit le rapport
- **Tri** : évaluation du contenu du rapport, catégorisation, prise de mesures préliminaires, hiérarchisation et gestion ;
- **Traité** : traitement du rapport, évaluation de l'exactitude de l'allégation, enquête en interne ou mesure de récupération de fonds ;
- **En cours d'investigation** - l'allégation fait l'objet d'une enquête ;
- **Clos** : fin du rapport ; conclusions possibles : soit aucune action n'est jugée nécessaire, soit l'enquête montre qu'aucune autre enquête n'est justifiée, soit le rapport est transféré pour un nouveau suivi, soit l'enquête est terminée (confirmant ou refusant l'infraction).

L'entreprise vise à traiter chaque rapport dans les meilleurs délais. Des circonstances telles que la complexité de l'infraction, conflit de priorités et d'autres raisons peuvent ralentir le traitement du rapport.

L'entreprise traite les rapports de manière confidentielle, impartiale et sans parti pris ni préjugé à faveur ou contre le lanceur d'alerte ou de toute autre personne impliquée dans l'infraction signalée, ou de tout témoin de celle-ci.

Les personnes affectées, c'est-à-dire les personnes accusées dans les rapports, bénéficient de la présomption d'innocence. Elles seront informées en temps utile. Toute enquête est menée de manière à préserver la confidentialité dans la mesure du possible et de manière appropriée afin que les personnes affectées ne soient pas exposées à une atteinte à leur réputation (l'information est partagée sur une base strictement confidentielle).

COMMUNICATION AVEC LES LANCEURS D'ALERTE

Une fois le rapport soumis, le lanceur d'alerte reçoit un accusé de réception dans un délai de sept jours maximum.

L'accusé de réception est envoyé à l'adresse électronique fournie par le lanceur d'alerte lors de la procédure d'envoi du rapport en ligne sur la plateforme de dénonciation Trusty. La confirmation de la réception du rapport est également dans la boîte de réception du lanceur d'alerte qui est accessible sur la plateforme Trusty, à l'aide des identifiants de connexion fournis au lanceur d'alerte lors de l'envoi du rapport. De la même façon, des identifiants sont fournis aux lanceurs d'alerte anonymes.

Si le rapport est soumis par le biais d'autres canaux de signalement internes disponibles, l'accusé de réception est envoyé aux coordonnées fournies par le lanceur d'alerte.

Le personnel autorisé sera en contact avec le lanceur d'alerte et, si nécessaire, lui demandera des informations ou des preuves supplémentaires. Toute communication sera effectuée via la boîte de réception du lanceur d'alerte sur la plateforme Trusty, ou par d'autres canaux de communication convenus avec le lanceur d'alerte.

Le lanceur d'alerte recevra du feedback au plus tard dans les trois mois après la soumission du rapport. Le retour d'information comprend des informations sur les mesures envisagées ou prises en guise de suivi et sur les motifs de ce suivi. Le retour d'information peut être limité pour éviter de compromettre une enquête ou d'autres procédures judiciaires, ainsi qu'en raison de restrictions légales sur ce qui peut être communiqué au sujet du suivi et des conclusions. Dans ce cas, et dans la mesure du possible, le lanceur d'alerte est informé des raisons de cette limitation de l'information.

L'entreprise peut décider de reconnaître et d'honorer le lanceur d'alerte pour avoir signalé une infraction, avec le consentement préalable de ce dernier (y compris, mais sans s'y limiter, l'expression de gratitude et les félicitations publiques de la part de la direction générale).

COMMENT PROTÉGER LES LANCEURS D'ALERTE CONTRE LES REPRÉSAILLES ?

INTERDICTION DE REPRÉSAILLES

Par représailles, on entend toute menace, proposition ou action réelle, directe ou indirecte, ou toute omission qui se produit dans un contexte professionnel, qui est motivée par un rapport interne ou externe ou par une divulgation publique, et qui cause ou peut causer un préjudice injustifié au lanceur d'alerte.

Les représailles peuvent inclure, entre autres, les mesures suivantes :

- suspension, mise à pied, licenciement ou mesures équivalentes ;
- dégradation ou refus de promotion ;
- transfert de fonctions, changement de lieu de travail, réduction de salaire, modification des horaires de travail ;
- refus de formation ;
- évaluation négative des performances ou des références d'emploi ;
- imposition ou administration d'une mesure disciplinaire, d'un blâme ou d'une autre sanction, y compris une sanction financière ;
- coercition, intimidation, harcèlement ou ostracisme, isolement ; discrimination, traitement défavorable ou injuste ;
- révélation d'identité du lanceur d'alerte.

Suite à la page suivante.

INTERDICTION DE REPRESAILLES (SUITE)

- refus de transformation d'un contrat temporaire en contrat à durée indéterminée, au détriment des attentes légitimes du salarié
- non-renouvellement ou résiliation anticipée d'un contrat de travail temporaire ;
- le préjudice, y compris la réputation de la personne, en particulier dans les médias sociaux, ou la perte financière, y compris la perte d'activité et la perte de revenus ;
- l'inscription sur une liste noire sur la base d'un accord informel ou formel à l'échelle d'un secteur ou d'une industrie, ce qui peut signifier que la personne ne trouvera plus d'emploi à l'avenir dans le secteur ou l'industrie en question ;
- la résiliation anticipée ou l'annulation d'un contrat de biens ou de services ;
- annulation d'une licence ou d'un permis ;
- allusions à des problèmes psychiatriques ou médicaux.

L'entreprise applique une politique de tolérance zéro aux possibles représailles. Toute forme de représailles, y compris les menaces et les tentatives de représailles, est interdite et doit être signalée immédiatement. Ces rapports peuvent être soumis en utilisant le canal de signalement interne de l'entreprise.

Toute personne se livrant à des représailles s'expose à de graves conséquences internes - et potentiellement externes - en vertu de la législation ou de la réglementation en vigueur. Si l'entreprise identifie une personne impliquée dans des représailles, celle-ci fera l'objet d'une action disciplinaire pouvant aller jusqu'au licenciement.

Toute infraction, mauvaise conduite, mauvaise gestion ou objectifs manqués par le lanceur d'alerte ne seront pas considérées comme représailles si elles ne gardent pas de relation avec le rapport d'alerte.



PROTECTION CONTRE LES REPRÉSAILLES

L'entreprise prendra toutes les mesures raisonnables pour protéger les lanceurs d'alerte contre les représailles.

Si des représailles ont été identifiées au sein de l'entreprise, celle-ci prendra les mesures nécessaires pour y mettre fin et soutenir le lanceur d'alerte. Si des mesures correctives sont nécessaires, l'entreprise doit, dans la mesure du possible, réintégrer le lanceur d'alerte dans la situation où il aurait pu être s'il n'avait pas subi de représailles. Par exemple :

- réintégrer le lanceur d'alerte dans le même poste ou à un poste équivalent, avec un salaire égal, des responsabilités égales, un poste de travail égal et une réputation égale.
- accès équitable à la promotion, à la formation, aux opportunités, aux avantages et aux droits ;
- rétablissement de la position commerciale antérieure par rapport à l'organisation ;
- retrait du litige ;
- présentation d'excuses pour tout préjudice subi ;
- indemnisation des dommages subis.

Après le signalement, le personnel autorisé évalue le risque potentiel de représailles contre le lanceur d'alerte et met en œuvre les stratégies et les actions nécessaires visant à les prévenir. Pour ce faire, le personnel autorisé identifie et met en œuvre des stratégies et des actions visant à prévenir de telles représailles ou à contenir les actes de représailles identifiés afin d'éviter d'autres préjudices, par exemple :

Suite à la page suivante.

PROTECTION CONTRE LES REPRESAILLES (SUITE)

- protection de l'identité du lanceur d'alerte ;
- partage d'information uniquement stricte et nécessaire ;
- communication régulière avec le lanceur d'alerte ;
- soutien émotionnel, financier, juridique ou en matière de réputation tout au long du processus ;
- encouragement au lanceur d'alerte de l'intérêt de signaler l'infraction et prendre des mesures pour contribuer à son bien-être ;
- modification du lieu de travail ou des modalités de signalement ;
- avertissement aux personnes concernées ou d'autres parties intéressées qu'un comportement de représailles ou une violation de la confidentialité peut constituer une infraction disciplinaire.

Le personnel autorisé surveille et examine les risques à différents stades de la procédure, notamment lorsque la décision d'enquêter est prise, pendant l'enquête sur le signalement et une fois que le résultat de l'enquête est connu, ainsi que, le cas échéant, après la clôture du cas.

Les protections prévues par la présente politique s'appliquent au lanceur d'alerte même si l'infraction signalée n'est pas corroborée, si le lanceur d'alerte avait des motifs raisonnables de croire que les informations sur l'infraction signalée étaient vraies au moment du signalement. De même, les lanceurs d'alerte qui ont signalé ou divulgué publiquement des informations sur des infractions de façon anonyme, mais qui sont par la suite identifiés et subissent des représailles, peuvent bénéficier de la protection prévue par la présente politique.

Toute personne qui fait sciemment de fausses déclarations s'expose à des mesures disciplinaires et/ou à d'autres actions en justice, pouvant aller jusqu'au licenciement.

COMBIEN DE TEMPS SE GARDENT LES RAPPORTS ?

Si le personnel autorisé ne corrobore pas l'infraction signalée et les données correspondantes ne sont pas requises par l'entreprise pour d'autres procédures, le rapport et toutes les informations recueillies liées au rapport et à son traitement sont définitivement supprimés après la clôture de l'affaire et l'expiration de la période de conservation définie dans un document distinct.

Si une infraction signalée est avérée, le rapport et toutes les informations recueillies liées au rapport et à son traitement seront conservés aussi longtemps que nécessaire pour faire valoir et exercer les droits légaux respectifs, ou pour se défendre contre ceux-ci.