www.smt.network

POLITIQUE DE SIGNALEMENT

SMT

20 avril 2023

INFORMATIONS SUR LE DOCUMENT

Auteur(s)	:	Département Legal & Compliance
Sujet	:	Politique de signalement
Version	:	1
Date	:	20 avril 2023

Revision	Date	Author(s)	Adjustment description	Check	Appr.

Sommaire

Page

1 Objectif

L'objectif de cette politique est de fournir un ensemble de lignes directrices claires sur l'approche et la gestion du signalement d'actes illégaux (présumés), de comportements contraires à l'éthique, de fautes professionnelles ou d'autres préoccupations graves, par toute partie prenante interne ou externe qui a le droit de signaler des abus conformément aux règles applicables en la matière.

Toutes les parties prenantes doivent savoir qu'elles peuvent fournir des informations sur toute préoccupation sérieuse qu'elles ont, comprendre où elles peuvent signaler leurs préoccupations, savoir ce qui se passe après qu'elles aient fait un signalement, et s'assurer qu'elles se sentent en sécurité en faisant un signalement.

Chacun doit pouvoir faire un signalement de manière anonyme. Nous nous engageons à protéger l'identité des lanceurs d'alerte et ils n'auront à révéler leur identité que s'ils choisissent de le faire.

Nous nous engageons à protéger les lanceurs d'alerte, qui signalent des abus de bonne foi, contre les mesures de représailles.

2 Champ d'application

La politique de signalement s'applique à toutes les parties prenantes internes et externes qui ont des droits de signalement conformément aux règlements applicables en matière de signalement. Sont considérées comme des parties prenantes internes : les employés (y compris les expatriés), les administrateurs et les actionnaires. Sont considérées comme des parties prenantes externes : les anciens employés, les candidats, les indépendants, les contractants et les fournisseurs. On ne peut renoncer à aucun des droits et protections énoncés dans la présente politique par aucun accord, politique, formulaire ou condition d'emploi.

Si, dans l'une des juridictions où nous opérons, il existe des lois sur la protection des signalements qui offrent un niveau de protection plus élevé que ce qui est inclus dans la présente politique, la législation locale prévaudra.

3 Propriété

La politique de signalement est gérée par le comité de signalement (ou whistleblowing committee). Toute modification de la politique de signalement nécessite l'approbation préalable du comité de signalement.

4 Définitions

Comité de signalement
Le comité de signalement est composé du Head of Compliance Group, Head of Legal Group et HR Director Group de SMT Holding SA.

Agent indépendant du signalement
Le comité de signalement a désigné Lighthouse Compliance Consultants comme agent indépendant de signalement (Independent Wistleblowing Officer = « **IWO** »). Il sera le seul destinataire des signalements. Cela garantit la confidentialité du lanceur d'alerte.

Système de signalement
Nous utilisons un système tiers crypté conforme à la norme ISO 27000 afin de permettre aux parties prenantes de signaler, de manière nominative ou anonyme, tout type d'acte illégal, de comportement contraire à l'éthique, de faute professionnelle ou d'autres préoccupations graves. Le système de gestion des signalements est disponible sur: https://SMT.safewhistleblowing.solutions

5 Processus de signalement

5.1 Quels types de comportement doivent être signalés ?

Il n'est pas de notre intention de limiter les sujets de préoccupations graves à signaler : en principe, toute forme de préoccupation grave peut être signalée, à condition que cela soit fait de bonne foi. Par conséquent, les catégories suivants d'actes illégaux (présumés), de comportements contraires à l'éthique, de fautes professionnelles et autres préoccupations graves doivent être signalés immédiatement :

- Fraude et détournement d'actifs ;
- Pots-de-vin et corruption ;
- Collusion et conflits d'intérêts ;
- Chantage ;
- Non-respect des lois antitrust ou de la concurrence ;
- Vol de données et fuite de données ;
- Espionnage d'entreprise ;
- Violation des règles comptables/des droits des actionnaires ;
- Problèmes d'environnement, de santé et de sécurité ;

- Comportement contraire à l'éthique, y compris harcèlement ou intimidation de toute nature ;
- Non-respect des règlements internes ; et
- Autres problèmes graves.

Le système de signalement ne doit pas être utilisé pour signaler des préoccupations quotidiennes dans la mesure où elles ne peuvent être qualifiées d'actes illégaux, de comportements non éthiques, de fautes ou d'autres préoccupations graves. Le système de signalement ne doit pas être utilisé par les employés pour soulever des griefs dits « de routine » concernant leur situation professionnelle personnelle.

Les préoccupations sérieuses peuvent être signalées même sans preuves à l'appui ; en effet, des soupçons raisonnables que des actes répréhensibles ont eu lieu, ont lieu ou sont sur le point d'avoir lieu étant suffisants.

Si vous avez signalé un problème grave en toute bonne foi, le processus et toutes les personnes impliquées dans sa mise en œuvre soutiendront et protégeront le lanceur d'alerte. Toutefois, si une fausse inquiétude est soulevée de mauvaise foi (par exemple, pour des raisons malveillantes ou sur la base de fausses déclarations), le lanceur d'alerte peut faire l'objet d'une action disciplinaire, conformément aux règles et politiques applicables, pouvant aller jusqu'au licenciement, ainsi que d'une saisine des autorités judiciaires.

5.2 Comment faire un signalement?

Si une partie prenante souhaite faire un signalement, elle peut utiliser le système d'alerte sécurisé qui permet de faire un signalement écrit nominatif ou anonyme, via la plateforme https://SMT.safewhistleblowing.solutions. Vous y trouverez plus de détails sur le processus de signalement.

Les lanceurs d'alerte basés dans l'UE peuvent également s'adresser directement aux autorités compétentes désignées par l'État membre de l'UE où le signalement a lieu. Dans le cas où le lanceur d'alerte fait usage de son droit d'informer les autorités compétentes, il lui est conseillé de le faire en utilisant un courrier crypté envoyé par WIFI privé, afin d'éviter l'interception des données par des tiers ou leur fuite. Nous recommandons néanmoins à la partie prenante de d'abord faire un signalement interne en utilisant le système de signalement sécurisé.

5.3 Garantie de protection de l’identité

L'IWO agira en tant qu‘administrateur de la protection de l'identité du lanceur d’alerte. L'IWO ne révélera pas l'identité du lanceur d’alerte sans son approbation préalable. Avant que cette approbation n'ait été obtenue, le contenu du signalement ne peut être partagé qu'avec le comité de signalement.

L'IWO organisera l'accès aux détails du signalement pour toutes les autres fonctions internes et les parties externes. Afin de garantir la confidentialité des signalements, l'accès aux détails du signalement pour les autres fonctions internes et les parties externes n'est possible que sur demande du comité de signalement et après avoir reçu l'approbation préalable du lanceur d’alerte.

Le lanceur d’alerte peut rester anonyme tout au long de l'évaluation du signalement. À tout moment, le lanceur d’alerte peut s'identifier, mais à aucun moment il ne sera contraint de le faire. Il convient de noter que nous ferons tout notre possible pour enquêter sur tous les signalements recevables, mais dans certains cas, il y a des limites à ce qui peut être réalisé si le lanceur d’alerte décide de rester anonyme. Si le lanceur d’alerte décide de divulguer son identité, les questions soulevées seront traitées dans la plus stricte confidentialité et feront l'objet d'une enquête discrète.

5.4 Garantie de protection contre les représailles

Nous prendrons les mesures nécessaires pour interdire toute forme de représailles à l'encontre des dénonciateurs (y compris les menaces et les tentatives de représailles), notamment - mais sans s'y limiter - sous la forme de :

- suspension, rétrogradation ou refus de promotion et refus de formation ;
- d'une évaluation négative des performances ou d'une référence d'emploi ;
- d'une mesure disciplinaire, d'une réprimande ou de toute autre sanction ;
- coercition, intimidation, harcèlement, discrimination ou traitement injuste ;
- la non-conversion d’un contrat de travail temporaire en un contrat permanent, lorsque le travailleur avait des attentes légitimes de se voir offrir un emploi permanent ;
- le non-renouvellement ou la résiliation anticipée d'un contrat de travail temporaire ;
- préjudice, y compris à la réputation de la personne (notamment dans les médias sociaux) ou perte financière, y compris perte d'activité et perte de revenus ;
- la mise sur une liste noire sur la base d'un accord formel ou informel à l'échelle du secteur ou de l'industrie, qui peut avoir pour conséquence que la personne ne trouvera pas d'emploi dans ledit secteur ou industrie ; ou
- la résiliation ou l'annulation anticipée d'un contrat de biens ou de services.

Nous veillons à ce que les lanceurs d'alerte aient accès, le cas échéant, à des mesures de soutien. Nous prendrons les mesures appropriées conformément aux procédures internes contre toutes personnes physiques ou morales qui :

- entravent ou tentent d'entraver le signalement ;
- exercent des représailles contre les dénonciateurs ;
- engagent des procédures vexatoires contre les dénonciateurs ; et
- enfreignent l'obligation de préserver la confidentialité de l'identité des dénonciateurs.

Le lanceur d'alerte doit pouvoir faire des signalement d'actes illégaux, de fautes professionnelles et d'autres problèmes graves sans crainte de représailles. Un lanceur d'alerte est protégé contre toute mesure négative liée au signalement. Si la divulgation de l'identité du lanceur d'alerte est suivie d'une mesure négative, il peut demander au comité de signalement de prouver qu'il n'y a aucun lien entre le signalement et la mesure négative (renversement de la charge de la preuve).

Il est question de "risque sérieux de représailles" lorsque le lanceur d'alerte pense que les représailles sont proches ou imminentes. Dans ce cas, le lanceur d'alerte doit contacter l'IWO, qui informera ensuite le comité de signalement. Le comité de signalement décidera des mesures à prendre pour protéger le lanceur d'alerte contre le risque sérieux de représailles, et le lanceur d'alerte en sera informé. Bien que les lanceurs d'alerte soient invités à partager leurs idées sur les mesures utiles possibles pour éviter les représailles, le comité de signalement n'est pas obligé de les suivre.

Les autres parties qui pourraient être amenées à témoigner ou qui sont impliquées dans l'enquête (pour autant que les conditions légales soient remplies) seront protégées des représailles de la même manière que le lanceur d'alerte.

5.5 Comment évaluer un signalement?

Ci-dessous, veuillez trouver les différentes étapes qui seront déclenchées dès la réception d'un signalement :

- Le signalement (nominatif ou anonyme) est reçu ;
- L'IWO, en tant que destinataire unique de tous les signalements, notifie la réception du signalement dans un délai maximum de 7 jours ;
- L'IWO effectuera une évaluation initiale du signalement et interagira avec le lanceur d'alerte si des détails ou des clarifications supplémentaires sont nécessaires ;
- Le comité de signalement recevra l'évaluation de l'IWO ;

- Sur la base des recommandations formulées par l'IWO, le comité de signalement décidera des classifications de risque et des mesures de suivi ;
- Le lanceur d'alerte sera informé soit du rejet du signalement, soit du l'acceptation du signalement dans un délai de 1 mois après le signalement ; et
- Après la notification de l'acceptation du signalement, le signalement sera programmé pour un rapport de statut. Dans ce cas, le lanceur d'alerte recevra un rapport de statut dans un délai maximum de 3 mois après la réception du signalement, avec un aperçu des mesures de suivi et des résultats.

Si, après avoir reçu la décision de rejet du signalement ou le rapport de statut, le lanceur d'alerte n'est pas satisfait, il peut en référer à l'IWO, qui informera ensuite le comité de signalement. Sur la base des recommandations formulées par l'IWO, le comité de signalement décidera des mesures de suivi éventuelles, dont le lanceur d'alerte sera informé. Bien que les lanceurs d'alerte soient invités à partager leurs idées sur d'éventuelles mesures de suivi utiles, le comité de signalement n'est pas obligé de les suivre.

SMT

SERVICES MACHINERY TRUCKS

www.smt.network