Politique Lanceur d'alerte

Préambule

Metabo Belgium SA, dont le siège social est établi à Noordkustlaan, 2A, 1702 Grand-Bigard, enregistrée à la Banque Carrefour des Entreprises sous le numéro 0469.601.051, ci-après dénommée « l'Entreprise », entend mener ses activités avec intégrité et éthique et, par conséquent, de fournir la possibilité de signaler, dans les termes et conditions décrits ci-dessous, toute violation des dispositions légales et réglementaires mentionnées à l'article 1 de cette Politique Lanceur d'alerte (ci-après dénommée « la Politique ») lorsqu'une telle violation est identifiée au sein de l'Entreprise.

À cette fin, l'Entreprise fournit les canaux de signalement établis au niveau de l'Entreprise et du Groupe KOKI (ci-après dénommé « le Groupe »). Le Groupe est conscient de sa responsabilité sociale dans l'ensemble de ses activités et la fonde sur les valeurs et principes éthiques généralement admis. La gestion durable est également un élément essentiel de la culture d'entreprise. Le Groupe applique ces principes et veille à leur respect.

Les canaux de signalement établis au niveau du Group sont régis par:

- les "*Rules of procedure for the whistleblowing procedure at Metabowerke GmbH*" (ci-après dénommées « *les Règles de procédure* »), mises à jour au fur et à mesure, disponibles sur le lien suivant : https://www.metabo.com/t3/fileadmin/metabo/com_en/030_company/Rules_of_Procedure.pdf

- la page https://www.metabo.com/be/nl/ et https://www.metabo.com/be/fr/ expliquant les différents canaux de signalement existants au travers desquels des rapports peuvent être introduits.

- la page https://koki-group-eu.integrityline.app/ via laquelle un signalement peut être introduit en ligne.

- toute autre Politique/Règle concernant les lanceurs d'alerte, qui sera rendue disponible.

Dans la mesure où cette Politique s'applique à l'Entreprise, cette Politique prime sur les règles établies par les Règles de procédure.

L'objet de cette Politique est d'encourager tous les membres du personnel et toute personne ayant une relation contractuelle avec l'Entreprise à divulguer, conformément aux termes et conditions établis par cette Politique, tout acte répréhensible, illégal, contraire à l'éthique ou frauduleux en lien avec les activités de l'Entreprise, sans crainte de faire l'objet de représailles. Dans cette Politique, l'Entreprise décrit la procédure qu'elle recommande de suivre en cas de suspicion de violation et précise la protection garantie aux lanceurs d'alerte.

Dans ce cadre, l'Entreprise s'engage à respecter la Directive 2019/1937 du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union, la loi belge qui la transpose (ci-après dénommée « *la Loi belge relative aux lanceurs d'alerte* »[1]), et :

- à permettre le signalement confidentiel, anonyme ou non, de toute information relative à un acte répréhensible potentiel ou effectif ;
- à fournir un niveau élevé de protection aux personnes qui effectuent un signalement ;

[1] La loi du 28 novembre 2022 sur la protection des personnes qui signalent des violations au droit de l'Union ou au droit national constatées au sein d'une entité juridique du secteur privé.

- à déterminer la procédure à suivre par la personne qui effectue un signalement (ci-après dénommée « *le lanceur d'alerte* ») ;
- à prendre les mesures de suivi vis-à-vis des comportements inappropriés au sein de l'Entreprise.

Cette Politique est disponible sur le site internet de l'Entreprise https://www.metabo.com/be/nl et https://www.metabo.com/be/fr/.

Article 1. Champ d'application matériel – quelles violations peuvent être signalées ?

1.1.
Les canaux de signalement de l'Entreprise et du Groupe permettent de signaler des violations présumées dans les domaines suivants déterminés par la Loi belge relative aux lanceurs d'alerte :

- Marchés publics
- Services, produits et marchés financiers et prévention du blanchiment de capitaux et du financement du terrorisme
- Sécurité et conformité des produits
- Sécurité des transports
- Protection de l'environnement
- Radioprotection et sûreté nucléaire
- Sécurité des aliments destinés à l'alimentation humaine et animale, santé et bien-être des animaux
- Santé publique
- Protection des consommateurs
- Protection de la vie privée et des données à caractère personnel et sécurité des réseaux et des systèmes d'information
- Lutte contre la fraude fiscale
- Lutte contre la fraude sociale

En outre, les violations portant atteinte aux intérêts financiers de l'Union peuvent être signalées, comme les violations relatives au marché intérieur européen, y compris les violations des règles de l'Union en matière de concurrence et d'aides d'État.

Une violation est définie comme un acte ou une omission qui est illicite ou va à l'encontre de l'objet ou de la finalité des règles prévues dans les domaines visés ci-dessus. Cela inclut toute violation d'une des dispositions légales ou réglementaires pertinentes ainsi que toute violation des dispositions adoptées en exécution des dispositions précitées.

1.2.
Par ailleurs, et compte tenu de l'engagement de l'Entreprise et du Groupe de mener leurs activités avec intégrité et éthique, et d'être informés de toute violation perpétrée dans le cadre de ces activités, l'Entreprise inclut les domaines supplémentaires suivants au champ d'application de la présente Politique :

- Violations des lois et des exigences réglementaires
- Violations des politiques et lignes directrices
- Violations de ses Codes de conduite
- Indices de corruption et de pots-de-vin
- Violations en matière de santé et de sécurité au travail
- Indices d'intimidation, de discrimination et de harcèlement
- Notes relatives à la comptabilité et à la tenue des livres
- Violations du droit de la concurrence et du droit antitrust

- Violations des droits humains
- Violations des contrôles du commerce international
- Conflits d'intérêts
- Divers

Les canaux de signalement ne permettent pas d'introduire des plaintes générales, des plaintes de clients ou des demandes de garanties.

Article 2. Champ d'application personnel – qui peut signaler des violations ?

Les canaux de signalements de l'Entreprise et du Groupe visent à traiter les signalements opérés par les personnes suivantes (« *les lanceurs d'alerte* ») lorsqu'elles ont obtenu des informations sur des violations dans un contexte professionnel :

- Les personnes ayant le statut de travailleurs ;
- Les personnes ayant le statut de travailleurs indépendants ;
- Les actionnaires et les membres de l'organe d'administration, de direction ou de surveillance d'une entreprise, y compris les membres non exécutifs, ainsi que les bénévoles et les stagiaires rémunérés ou non rémunérés ;
- Les personnes travaillant sous la supervision et la direction de contractants, de sous-traitants et de fournisseurs ;
- Les personnes qui signalent des informations sur des violations obtenues dans le cadre d'une relation de travail qui a pris fin depuis ;
- Les personnes dont la relation de travail n'a pas encore commencé dans les cas où des informations sur des violations ont été obtenues lors du processus de recrutement ou d'autres négociations précontractuelles ;
- Les personnes qui détiennent des informations qu'ils ont obtenues en dehors d'un contexte professionnel concernant des violations commises au sein de l'Entreprise en matière de services, produits et marchés financiers.

Article 3. Le signalement

Toute personne visée à l'article 2 peut signaler, via l'un des canaux de signalement visés ci-après, des informations, y compris des soupçons raisonnables, concernant des violations effectives ou potentielles ou des risques y relatifs, qui se sont produites ou sont très susceptibles de se produire ainsi que concernant des tentatives de dissimulation de telles violations.

Les violations sont définies comme des actes ou omissions qui sont illicites et concernent l'un des domaines visés à l'article 1 ou qui vont à l'encontre de l'objet ou de la finalité des règles prévues dans les domaines visés à l'article 1.

Article 4. Canaux de signalement

Toute personne visée à l'article 2 qui a connaissance de ou des motifs raisonnables de soupçonner une violation au sein de l'Entreprise dans les domaines visés à l'article 1 est invitée à les signaler directement via les canaux de signalement.

4.1. Canaux de signalement internes

4.1.1. Canaux de signalement internes disponibles

Les canaux de signalement suivants permettent aux lanceurs d'alerte d'opérer des signalements au niveau de l'Entreprise et du Groupe :

En ligne	https://koki-group-eu.integrityline.app/
Par voie postale	CONFIDENTIEL Metabo Belgium SA Compliance Officer Noordkustlaan 2A 1702 Grand Bigard Belgique

Le lanceur d'alerte peut choisir le canal de signalement qu'il souhaite utiliser pour effectuer son signalement.

Si le lanceur d'alerte souhaite effectuer un signalement anonymement[2], il lui est recommandé d'utiliser le système de signalement en ligne[3]. Des communications anonymes avec le lanceur d'alerte sont également possibles via le système de signalement en ligne. L'Entreprise recommande donc aux lanceurs d'alerte qui utilisent le système de signalement en ligne de se connecter régulièrement à la plateforme et de vérifier si de nouveaux messages se trouvent dans le dossier de leur signalement.

Les signalements opérés via le système de signalement en ligne sont gratuits. En cas de signalement par la poste, le lanceur d'alerte peut décider de laisser ou non ses coordonnées.

Si un signalement concerne une société du Groupe en particulier, le lanceur d'alerte peut sélectionner celle-ci dans le système de signalement en ligne et ainsi permettre au signalement d'être traité par cette société.

Le canal de signalement est conçu, établi et géré de manière sécurisée qui garantit la confidentialité de l'identité du lanceur d'alerte et de tout tiers mentionné dans le signalement et qui empêche l'accès auxdits canaux par des membres du personnel non autorisés. Le canal assure à tout moment la protection de la vie privée et des données à caractère personnel du lanceur d'alerte ainsi que celles de tout tiers mentionné dans le signalement.

4.1.2. Traitement des signalements

A. Notification

Le lanceur d'alerte doit se rendre sur la page d'accueil et cliquer sur le bouton « faire un signalement ».

Sur la page suivante, le lanceur d'alerte formule son signalement dans ses propres mots et répond aux questions concernant la situation qu'il a observée (sélectionner une réponse ou entrer son propre texte).

---

[2] Nous encourageons cependant le lanceur d'alerte à mentionner son nom dans son signalement.

[3] Comment l'anonymat du lanceur d'alerte est-il protégé ?
Lorsqu'il soumet un signalement ou une question via la Ligne Intégrité, le lanceur d'alerte reste anonyme à moins qu'il ne décide de révéler son identité. Dans la mesure où le lanceur d'alerte n'introduit pas lui-même de données qui peuvent permettre de déduire son identité, le système protège son anonymité grâce à des moyens techniques certifiés.
Son signalement reste anonyme grâce au cryptage et à d'autres moyens de sécurité. En outre, le système ne stocke pas les adresses IP et les identifiants de l'ordinateur et n'utilise pas de cookies. Cependant, si un signalement est créé à partir d'un ordinateur du réseau de l'entreprise, il existe un risque que les sites internet visités soient enregistrés par le navigateur ou dans l'historique de l'entreprise. Afin d'éliminer ce risque, le lanceur d'alerte peut créer un signalement à partir d'un ordinateur qui ne fait pas partie du réseau de l'entreprise. Si le lanceur d'alerte télécharge des documents, il doit également être conscient que les fichiers peuvent contenir des métadonnées qui peuvent révéler l'identité du lanceur d'alerte. Par conséquent, il devrait s'assurer que toute métadonnée soit supprimée des fichiers avant de les télécharger.

Il peut également joindre un fichier à l'appui de son signalement ou enregistrer un extrait sonore. Le lanceur d'alerte doit garder à l'esprit que les fichiers peuvent contenir des informations concernant leur auteur (métadonnées).

Le lanceur d'alerte peut soumettre un signalement en utilisant son nom ou de manière anonyme. Ensuite, le lanceur d'alerte doit configurer sa propre boite e-mail sécurisée[4] (voir « Boite de réception sécurisée »). Cette boite e-mail permettra au lanceur d'alerte de recevoir un retour d'information et de pouvoir répondre aux questions que nous pourrions avoir.

Le lanceur d'alerte sera ensuite amené à répondre à une question de sécurité pour prouver qu'il n'est pas un « robot ».

B. Contenu du signalement

Les signalements devraient contenir les informations suivantes :

- Quel est votre soupçon (Description de l'incident – ce qui est arrivé, quand et où, l'incident est-il toujours en cours, etc.) ?
- Au sein de quelle société l'incident s'est-il produit ?
- Où l'incident s'est-il produit (pays, ville, évènement, etc.)
- Le lanceur d'alerte est-il un travailleur de la société concernée, un fournisseur, un consommateur, etc. ?
- Quel est le nom du département concerné ?
- Qui est impliqué dans l'incident (personne potentiellement suspecte) ?
- Quelqu'un a-t-il observé l'incident (témoins) ?
- Y a-t-il des preuves de l'incident (part exemple, des documents, etc.) ?

C. Qu'advient-il après le signalement ?

▪ Destinataire du signalement

Tous les signalements sont envoyés via des serveurs sécurisés du canal de signalement en ligne au *Chief Compliance Officer* de Metabowerke GmbH et ses représentants et/ou, le cas échéant, au Compliance Officer responsable au niveau local ou régional et ses représentants. Ils agissent en toute indépendance, confidentiellement et sans conflits d'intérêts ou instructions.

Si le Chief Compliance Officier de Metabowerke GmbH, ses représentants, le Compliance Officer responsable au niveau local ou régional et ses représentants ou d'autres travailleurs se trouvent en situation de conflit d'intérêts ou si la violation qui fait l'objet du signalement a été commise par l'une de ces personnes elles-mêmes, cette personne sera immédiatement mise à l'écart de l'enquête.

▪ Accusé de réception

[4] Via la boite e-mail sécurisée, nous mettons à la disposition du lanceur d'alerte un espace technique qui n'est accessible qu'au lanceur d'alerte et l'Entreprise. L'Entreprise peut contacter le lanceur d'alerte via cette boite e-mail sécurisée. C'est important, car des questions émergent souvent au cours du traitement du signalement que l'Entreprise peut uniquement éclaircir avec l'aide du lanceur d'alerte et qui peuvent être décisives pour la suite de la procédure.
Lorsque le lanceur d'alerte crée une boite e-mail sécurisée, il se verra attribuer un numéro d'identification de dossier et devra choisir un mot de passe. Le lanceur d'alerte doit utiliser ce numéro d'identification de dossier et ce mot de passe pour accéder à la boite e-mail et vérifier s'il a reçu des questions. Via cette boite e-mail sécurisée, l'Entreprise communiquera un retour d'information sur ce qu'il advient du signalement.
Si le lanceur d'alerte le souhaite, toutes les communications avec l'Entreprise resteront anonymes.

Le lanceur d'alerte reçoit un accusé de réception du signalement dans un délai de 7 jours à compter du jour de la réception du signalement s'il a fourni ses coordonnées ou s'il a mis en place une option de communication.

- **Suivi du signalement**

  - **Vérification du signalement**

Un suivi du signalement sera effectué par le destinataire du signalement.

Le « suivi » signifie toute mesure prise par le destinataire du signalement afin d'évaluer l'exactitude (/la recevabilité) des allégations formulées dans le signalement (c'est-à-dire si un signalement opéré est couvert par le champ d'application défini ci-dessus, si ce n'est pas le cas, le lanceur d'alerte reçoit un retour d'information en ce sens) et, le cas échéant, afin de remédier à la violation signalée, notamment par les mesures telles que :

- Une enquête (interne) ;
- Des poursuites ;
- une action en recouvrement de fonds ;
- ou la clôture de la procédure (si, en évaluant l'exactitude (/la recevabilité) du signalement, le destinataire du signalement arrive à la conclusion que l'incident ne peut pas être signalé via le système de lancement d'alerte).

  - **Clarification des faits**

Le destinataire du signalement reste en contact avec le lanceur d'alerte afin de lui fournir un retour d'information et de pouvoir lui demander des informations supplémentaires si nécessaire, par exemple, si les faits doivent être clarifiés (dans ce cas, le destinataire du signalement contactera le lanceur d'alerte via la Ligne Intégrité ou via d'autres moyens de communication, s'ils sont mis à disposition par le lanceur d'alerte).

Il peut être nécessaire de faire appel à d'autres services spécialisés, tels que les ressources humaines, la protection des données, les achats, etc. ou à des prestataires de services externes.

Si nécessaire, il peut être fait appel aux autorités répressives, ce qui pourra en particulier être le cas lorsqu'il existe une obligation légale de le faire ou si des éclaircissements supplémentaires concernant les faits ne sont plus possibles via des mesures internes bien qu'ils apparaissent nécessaires.

Dans le cas de signalement concret d'activités suspectes, il pourra être fait appel à des spécialistes et une enquête pourra être ouverte.

- **Enquête**

Si le signalement est confirmé, il fera l'objet d'une enquête rapide et approfondie conformément à la présente Politique. Toutes les investigations seront menées de manière approfondie, en tenant compte des principes de confidentialité, de protection des données, d'impartialité et d'équité vis-à-vis de l'ensemble des personnes concernées.

- **Mesures**

Les mesures appropriées seront examinées et, si nécessaire, adoptées et suivies.

Il peut s'agir de sanctions contre les travailleurs, telles qu'un avertissement, un blâme ou un licenciement, en tenant compte de la nature et de la gravité de la violation ainsi que de son caractère fautif ou intentionnel.

Si nécessaire, des poursuites pénales seront engagées. Des dommages et intérêts pourront également être réclamés.

Les mesures correctrices visent à prévenir ou faire cesser la violation ou, à tout le moins, la limiter s'il n'est pas possible de la prévenir ou de la faire cesser.

En outre, la nécessité d'adopter, d'étendre et de mettre en œuvre des mesures préventives sera évaluée.

D. Retour d'informations

Au plus tard 3 mois à compter de l'accusé de réception, ou, si aucun accusé de réception n'a été notifié au lanceur d'alerte, trois mois à partir de l'expiration d'un délai de 7 jours à compter du signalement, le lanceur d'alerte recevra un retour d'information sur les mesures qui sont envisagées ou qui ont été prises ainsi que sur les motifs du choix de ces mesures, si le lanceur d'alerte a fourni ses coordonnées ou a établi d'autres moyens de communication. Des informations confidentielles peuvent être communiquées afin de garantir un retour d'information.

E. Fin de la procédure - archivage

À la fin de la procédure, les résultats et les mesures prises sont documentés et stockés d'une manière qui en sécurise l'accès. Les obligations légales de suppression et de conservation sont respectées.

4.2. Canaux de signalement externe

Alternativement aux canaux de signalement interne de l'Entreprise et du Groupe, le lanceur d'alerte peut choisir d'effectuer un signalement concernant des suspicions de violations via les canaux de signalement externe, tels que ceux mis à disposition par les autorités belges compétentes[5], après avoir

[5] *1° le Service public fédéral Economie, PME, Classes Moyennes et Energie ;*
2° le Service public fédéral Finances ;
3° le Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement ;
4° le Service public fédéral Mobilité et Transports ;
5° le Service public fédéral Emploi, Travail et Concertation sociale ;
6° le Service public de programmation Intégration Sociale, Lutte contre la Pauvreté, Economie Sociale et Politique des Grandes Villes ;
7° l'Agence fédérale de Contrôle nucléaire ;
8° l'Agence fédérale des médicaments et des produits de santé ;
9° l'Agence fédérale pour la sécurité de la chaîne alimentaire ;
10° l'Autorité belge de la Concurrence ;
11° l'Autorité de protection des données ;
12° l'Autorité des services et marchés financiers ;
13° la Banque nationale de Belgique ;
14° le Collège de supervision des réviseurs d'entreprises ;
15° les autorités visées à l'article 85 de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces ;
16° le Comité national de sécurité pour la fourniture et la distribution d'eau potable ;
17° l'Institut belge des services postaux et des télécommunications ;
18° l'Institut National d'Assurance Maladie-Invalidité ;
19° l'Institut National d'Assurances Sociales pour Travailleurs Indépendants ;
20° l'Office National de l'Emploi ;
21° l'Office National de Sécurité Sociale ;

préalablement effectué un signalement via les canaux de signalement interne, ou en effectuant directement un signalement via les canaux de signalement externe.

Ces autorités sont désignées pour recevoir les signalements externes, donner un retour d'information au lanceur d'alerte, et exercer les missions prévues par la Loi belge relative aux lanceurs d'alerte, en particulier en ce qui concerne le suivi du signalement.

Les Médiateurs fédéraux sont chargés de coordonner les signalements opérés via le canal de signalement externe. En résumé, ils sont chargés de recevoir les signalements externes, vérifier leur recevabilité et les transmettre à l'autorité compétente pour enquêter sur ces signalements, en fonction de l'objet du signalement.

Si l'autorité qui a reçu un signalement n'est pas compétente pour traiter la violation signalée, cette autorité transmet le signalement aux Médiateurs fédéraux qui transmettent le signalement à l'autorité compétente, dans un délai raisonnable et de manière sécurisée.

Si aucune autorité ne s'estime compétente pour recevoir un signalement, les Médiateurs fédéraux agissent en tant qu'autorité compétente pour recevoir le signalement externe.

Les coordonnées du Médiateur fédéral sont les suivantes :

Adresse : Rue de Louvain, 48, boîte 6 1000 Bruxelles
Plainte en ligne : https://www.mediateurfederal.be / https://www.federaalombudsman.be
E-mail: contact@mediateurfederal.be / contact@federaalombudsman.be
Téléphone : 0800 99 961 ou +32 2 289 27 27 depuis l'étranger
Numéro de fax : +32 2 289 27 28

Nous vous recommandons de privilégier, à chaque fois que cela est possible, le recours aux canaux de signalement interne de l'Entreprise et du Groupe. En cas de signalement externe, les mesures protectrices contre les représailles sont uniquement octroyées si les conditions spécifiques prévues à l'article 5.2.3. sont rencontrées.

Article 5. Protection des lanceurs d'alerte

5.1. Confidentialité

L'identité du lanceur d'alerte est traitée de manière strictement confidentielle tout au long de la procédure et ne peut en aucun cas être divulguée à toute personne autre que (1) les personnes compétentes pour recevoir le signalement et assurer son suivi et autre que (2), à moins qu'une exception légale ne s'applique, la personne concernée par le signalement endéans un délai raisonnable, en raison des exigences en matière de protection des données, ne pouvant dépasser un mois à partir du signalement, sauf s'il existe une obligation légale de divulgation[6] ou si le lanceur d'alerte consent à ce que son identité soit divulguée.

22° le Service d'Information et de Recherche Sociale ;
23° le Service autonome de Coordination Anti-Fraude (CAF) ;
24° le Contrôle de la Navigation.

[6] L'identité du lanceur d'alerte peut être divulguée lorsqu'il s'agit d'une obligation nécessaire et proportionnée en vertu d'une législation spéciale dans le cadre d'enquêtes menées par des autorités nationales ou dans le cadre de procédures judiciaires, notamment en vue de sauvegarder les droits de la défense de la personne concernée (c'est-à-dire « une personne physique ou morale qui est mentionnée dans le signalement ou la divulgation publique en tant que personne à laquelle la violation est attribuée ou à laquelle cette personne est associée »). Dans cette hypothèse, le lanceur d'alerte sera informé avant que son identité ne soit divulguée, à moins qu'une telle information ne risque de compromettre les enquêtes ou les procédures judiciaires concernées.

Cela vaut également pour toute autre information à partir de laquelle l'identité du lanceur d'alerte peut être directement ou indirectement déduite.

Toutes les parties internes et externes impliquées dans l'enquête et le suivi du signalement sont liées par une obligation de confidentialité.

5.2. Protection contre les représailles

5.2.1. Personnes protégées

Toute forme de représailles est interdite vis-à-vis des personnes visées à l'article 2, en ce compris les menaces de représailles et tentatives de représailles, en raison des faits signalés. La protection contre les représailles bénéficie également aux personnes suivantes si elles disposaient de motifs raisonnables de penser que le lanceur d'alerte tombait dans le champ d'application de la Loi belge relative aux lanceurs d'alerte :

- Les facilitateurs
- Les tiers qui sont en lien avec les lanceurs d'alerte et qui risquent de faire l'objet de représailles dans un contexte professionnel, tels que des collègues ou des proches du lanceur d'alerte ; ainsi que
- Les entités juridiques appartenant aux lanceurs d'alertes ou pour lesquelles ils travaillent, ou encore avec lesquelles ils sont en lien dans un contexte professionnel.

Les représailles visent tout acte ou omission direct ou indirect suscité par un signalement interne ou externe ou une divulgation publique, et qui cause ou est susceptible de causer un préjudice injustifié au lanceur d'alerte.

5.2.2. Les représailles

À moins qu'elles ne soient dument justifiées, les mesures suivantes peuvent constituer des représailles :

- Les mesures liées à l'emploi, par exemple suspension, mise à pied, licenciement, réduction de salaire, refus de promotion, sanctions ou mesures disciplinaires, réprimande, ou autre sanction, y compris sanction financière, rétrogradation, refus de promotion, évaluation de performances ou attestation de travail basse ou négative ;
- Les décisions ayant des conséquences négatives sur les conditions de travail, par exemple transferts de fonctions, changement de lieu de travail, réduction de salaire, modification des horaires, refus de congé ;
- Certains comportements, par exemple coercition, intimation, harcèlement, ostracisme, traitement désavantageux ou injuste ;
- La non-conversion d'un contrat de travail temporaire en un contrat permanent, lorsque le travailleur pouvait légitimement espérer se voir offrir un emploi permanent ;
- Le non-renouvellement ou résiliation anticipée d'un contrat de travail temporaire ;
- Le préjudice, y compris les atteintes à la réputation de la personne, en particulier sur les réseaux sociaux, ou pertes financières, y compris la perte d'activité et la perte de revenu ;
- La mise sur liste noire sur la base d'un accord formel ou informel à l'échelle sectorielle ou de la branche d'activité, pouvant impliquer que la personne ne trouvera pas d'emploi à l'avenir au niveau du secteur ou de la branche d'activité ;
- La résiliation anticipée ou annulation d'un contrat relatif à la fourniture de biens ou la prestation de services ;
- L'exclusion ou la suspension d'un membre ou de son délégué désigné ;
- L'annulation d'une licence ou d'un permis ;

- L'orientation vers un traitement psychiatrique ou médical.

5.2.3. Les conditions de la protection - Que se passe-t-il si le contenu du rapport s'avère finalement faux ?

La protection contre les représailles est garantie à condition que les conditions suivantes soient respectées :

- Le lanceur d'alerte a agi de bonne foi au moment où le signalement a été effectué, cela signifie qu'il avait des motifs raisonnables de croire que les informations signalées sur les violations étaient véridiques au moment du signalement et que ces informations entraient dans le champ d'application de cette Politique.

- Le lanceur d'alerte doit avoir effectué son signalement conformément à la présente Politique et à la Loi belge relative aux lanceurs d'alerte.

Le respect de la première condition est évalué par rapport à une personne se trouvant dans une situation similaire et disposant de connaissances comparables. Il est important que le lanceur d'alerte croie ou suppose au moment où il opère son signalement que le contenu de celui-ci est véridique et qu'il ne soumet pas ce signalement avec une intention abusive. Il n'est pas attendu du lanceur d'alerte qu'il cherche des preuves ou clarifie l'incident par lui-même. Par conséquent, il se peut que l'enquête révèle finalement qu'il n'existe aucune violation. Dans ce cas, le lanceur d'alerte ne perd pas le bénéfice de la protection au seul motif que le signalement effectué de bonne foi s'est avéré inexact ou infondé.

En cas de signalement abusif, opportuniste ou effectué de mauvaise foi ou dans le cas où un signalement est fait dans le seul objectif de porter préjudice à l'Entreprise ou à de tierces parties, le lanceur d'alerte peut encourir des sanctions disciplinaires (y compris des sanctions prévues par le règlement de travail), des poursuites judiciaires et des sanctions pénales[7].

Il est interdit d'entraver un signalement. Toute personne qui entrave le signalement d'un lanceur d'alerte s'expose également à des sanctions disciplinaires (y compris des sanctions prévues par le règlement de travail), à des poursuites judiciaires ou à des sanctions pénales[8].

Article 6. La protection des données à caractère personnel

Les données à caractère personnel communiquées dans le cadre de la procédure de signalement sont traitées par Metabo Belgium SA, agissant en tant que responsable de traitement, ayant son siège social à Noordkustlaan, 2A, 1702 Grand-Bigard, inscrite à la Banque-Carrefour des Entreprises sous le numéro 0469.601.051.

L'Entreprise collecte et traite ces données à caractère personnel conformément à la législation sur la protection des lanceurs d'alerte, y compris la Loi belge relative aux lanceurs d'alerte, et la législation relative à la protection des données à caractère personnel, y compris le Règlement 2016/679 (le « RGPD »).

---

[7] Lorsqu'il peut être établi qu'une personne a sciemment signalé ou divulgué publiquement de fausses informations, celle-ci s'expose à des sanctions pénales en vertu des articles 443 à 450 du Code pénal belge, et pourra se voir réclamer des dommages et intérêts civils (cfr. art. 33, §3 de la Loi belge relative aux lanceurs d'alerte).

[8] Le fait d'empêcher une personne d'introduire un signalement ou de prendre des mesures de représailles est passible d'une peine d'emprisonnement de 6 mois à 3 ans et/ou d'une peine d'amende de 600 à 6000 euros. La sanction peut être prononcée à l'encontre de l'Entreprise et/ou des membres de son personnel (cfr. art. 33, §2 de la Loi belge relative aux lanceurs d'alerte).

Ce traitement des données à caractère personnel est effectué dans le cadre du respect d'une obligation légale et/ou de l'intérêt légitime de l'Entreprise, dans la mesure où le canal de signalement interne dépasse les objectifs légaux, en particulier la détection des crimes et la garantie d'une conduite sûre et éthique de l'Entreprise.

Les informations pertinentes relatives à la protection des données à caractère personnel sont disponibles sur le système de signalement en ligne:
https://koki-group-eu.integrityline.app/app-page;appPageName=Privacy%20policy?lang=nl
EQS Integrity Line

De plus amples informations concernant la protection des données à caractère personnel sont disponibles à l'adresse suivante :
https://www.metabo.com/be/fr/info/generalites/protection-des-donnees/
https://www.metabo.com/be/nl/info/algemeen/gegevensbescherming/

Article 7. Entrée en vigueur

Cette Politique entre en vigueur le 8 novembre 2025 pour une durée indéterminée.

L'Entreprise se réserve le droit de modifier cette Politique à tout moment, notamment, mais pas uniquement, en cas de modifications de la législation pertinente et/ou des exigences opérationnelles.