



Place de l'Albertine, 2
1000 Brussels - Belgium
+32 2 511 13 09
+32 2 511 42 13
jgi@jgi.be
www.jgi-hydrometal.be

Politique d'alerte professionnelle et de signalement (V25/01)

1. Introduction

Les règles de gestion de JGI (ci-après « l'employeur ») contiennent des valeurs fondamentales, des normes et des règles devant être respectées au sein de l'entreprise dans son ensemble dans le cadre des relations entretenues avec tous les contacts de l'employeur : clients, fournisseurs, actionnaires et collaborateurs.

JGI s'impose des exigences élevées en termes de transparence et d'intégrité. Dans ce contexte, l'employeur invite son personnel ou toute tierce personne ayant des préoccupations quant à une violation (présumée) du code de conduite de l'employeur ou des domaines du droit européen et belge énumérés au titre 3, à faire part de ces préoccupations sans crainte de représailles, telles que des sanctions et/ou un traitement injuste.

Afin de guider les collaborateurs dans cette démarche, un système d'alerte professionnelle a été élaboré. Ce système décrit la protection dont bénéficient les lanceurs d'alerte, ainsi que la manière dont une alerte peut être lancée et les suites qui seront données à celle-ci. L'employeur n'attend pas d'un lanceur d'alerte qu'il soit en mesure de prouver qu'une allégation est justifiée. En revanche, il doit pouvoir prouver qu'il existe des raisons suffisantes de considérer que quelque chose n'est pas normal.

La règle générale est que tout signalement ou tout soupçon de violation de l'intégrité soit d'abord discuté avec le responsable direct ou le supérieur hiérarchique. Si cela n'est pas possible ou si cela ne conduit pas à la réaction souhaitée, le lanceur d'alerte peut toujours contacter aussi la personne de confiance (interne/externe). Ce régime de notification n'affecte pas les règles relatives à l'exercice du droit de consulter le représentant des travailleurs ou les syndicats et la protection contre toute mesure défavorable injustifiée résultant de ces consultations.



Toutefois, lorsqu'il n'y a plus d'autre possibilité, pour quelque raison que ce soit, le lanceur d'alerte peut s'adresser au canal de signalement interne ou à un point de contact externe indépendant. Si cela n'est pas du tout envisageable non plus, le lanceur d'alerte peut rendre le soupçon de violation publique.

L'organisation du canal interne, les procédures à suivre pour le canal interne et le suivi des rapports seront mis en place après consultation des partenaires sociaux.

2. Définitions

Violation : des actes ou omissions qui soit :

- Sont illicites et concernent les domaines énumérés à l'article 3 "Champ d'application"
- Vont à l'encontre de l'objet ou de la finalité des règles relevant des champs d'application énumérés à l'article 3.

Les informations sur les violations : sont des informations, y compris des soupçons raisonnables, sur des violations effectives ou potentielles, qui se sont produites ou qui sont très susceptibles de se produire, ainsi que sur des tentatives de dissimulation de telles violations.

Lanceur d'alerte : une personne physique qui signale ou divulgue des informations sur des violations, oralement ou par écrit, et ce dans un contexte professionnel. Un contexte professionnel fait référence aux activités professionnelles actuelles ou passées dans le secteur privé par le biais desquelles, quelle que soit la nature de ces activités, des personnes peuvent obtenir des informations sur des violations et où ces personnes peuvent subir des représailles si elles devaient signaler ces informations.

Le lanceur d'alerte peut être un (futur) employé, un ex-employé, un prestataire de services indépendant, un bénévole, un stagiaire (non) rémunéré, un (employé d'un) client, un fournisseur ou un (sous-)contractant, un actionnaire, une personne appartenant à l'organe d'administration, de gestion ou de surveillance d'une entreprise ou toute tierce personne qui, dans un contexte professionnel, a obtenu des informations sur une éventuelle violation qu'elle souhaite signaler.

Facilitateur : une personne physique qui assiste le lanceur d'alerte dans le processus de déclaration et dont l'assistance doit être confidentielle.

Personne concernée : Une personne physique (par exemple, un collègue) ou morale (par exemple, une entreprise) nommée dans le signalement ou la divulgation publique comme étant une personne à qui la violation est attribuée ou avec laquelle cette personne est associée.

Gestionnaire de signalement : la personne ou le service impartial habilité à assurer le suivi des signalements d'infraction, à maintenir la communication avec le lanceur d'alerte, à lui demander des informations complémentaires si nécessaire, à lui fournir un retour d'information et, le cas échéant, à recevoir et traiter les signalements.

Auditeur interne : toute personne qui exerce la fonction d'audit interne pour l'employeur.

Représailles : acte ou omission directe ou indirecte en réponse à un signalement interne ou externe ou une divulgation publique, et qui entraîne ou peut entraîner un préjudice injustifié pour le lanceur d'alerte.



3. Champ d'application

Dans le cadre de ce système, une distinction est faite entre l'intégrité sociale et l'intégrité professionnelle.

Les violations d'intégrité sociale couvrent les comportements indésirables tels que le harcèlement, la discrimination fondée sur le genre, l'âge, le handicap, l'orientation, la vie sexuelle, l'origine raciale ou ethnique, les convictions religieuses ou philosophiques, l'intimidation sexuelle, la violence, ... Cela nécessite une approche différente. Bien que l'employeur considère ceux-ci comme un comportement non intègre, ils ne relèvent pas du champ d'application spécifique de la législation sur le lancement d'alertes.

Les violations de l'intégrité professionnelle, en revanche, comme précisées ci-dessous, concernent, entre autres, la manière dont sont gérées les informations confidentielles, le matériel et les biens, la santé et la sécurité ainsi que les relations avec les clients (potentiels) et fournisseurs. Les comportements professionnels non intègres incluent également les infractions comptables, financières et bancaires ainsi que les violations des règles en matière d'audit, de corruption et de concurrence.

La différence entre les deux types de comportements est que, dans le cas d'un comportement social indésirable, il y a souvent un plaignant et un accusé, tous deux directement identifiables, entre lesquels le comportement indésirable se produit, tandis que les problèmes d'intégrité professionnelle peuvent être signalés sans que le lanceur d'alerte (ex : en tant que victime) ne soit forcément impliqué directement. Dans la pratique, la limite entre intégrité sociale et intégrité professionnelle n'est pas toujours claire. On peut toutefois partir du principe que les comportements indésirables de type social sont avant tout dirigés contre un individu tandis que les autres violations de l'intégrité sont dirigées contre (les intérêts de) l'organisation propre, des organisations externes ou la société dans son ensemble.

Les violations de l'intégrité professionnelle concernent les domaines suivants de la législation européenne et belge :

- Marchés publics ;
- Services, produits et marchés financiers, prévention du blanchiment d'argent et du financement du terrorisme ;
- Sécurité et conformité des produits ;
- Sécurité des transports ;
- Protection de l'environnement ;
- Radioprotection et sûreté nucléaire ;
- Sécurité des denrées alimentaires et des aliments pour animaux, santé animale et bien-être des animaux ;
- La santé publique ;
- Protection des consommateurs ;

- Protection de la vie privée et des données personnelles, et sécurité des réseaux et des systèmes d'information ;
- Les infractions relatives au marché intérieur de l'Union européenne, telles que les violations des règles relatives aux aides d'État et à la concurrence : comportements et accords anticoncurrentiels, abus de prix, abus de position dominante, etc. ;
- Fraude fiscale ;
- Lutte contre la fraude sociale ;
- Infractions portant atteinte aux intérêts financiers de l'Union européenne ;
- Santé et sécurité au travail : violence au travail, notamment sous la forme de pressions exercées sur les travailleurs pouvant avoir des conséquences physiques et psychologiques néfastes, non-respect des obligations applicables en cas d'accidents du travail et de maladies professionnelles, mise en danger de travailleurs, exposition des travailleurs à des produits dangereux, conditions de travail, installations et outils non conformes, pouvant porter atteinte à la santé, la sécurité et l'hygiène des travailleurs ;
- Corruption, en particulier concernant les activités de l'employeur : faux certificats et autres violations de l'intégrité de l'employeur.

Ce sont les signalements concernant les violations mentionnées ci-dessus qui doivent se faire selon la procédure décrite ci-dessous afin de bénéficier d'une protection juridique contre les représailles.

4. Signalement et étapes suivantes

4.1. Choisir le canal de signalement le plus approprié

Plusieurs options se présentent à un lanceur d'alerte pour signaler une violation. Les violations de l'intégrité sociale et interpersonnelle doivent être signalées par les trois premiers canaux cités.

Les méthodes 4, 5 et 6 sont spécifiquement fournies dans le contexte de violations d'intégrité professionnelle dans le cadre de la loi sur les lanceurs d'alerte et ne peuvent être utilisées que dans ce contexte.

1. Il est préférable de signaler une infraction (présumée) à la ligne hiérarchique (n+1) en premier lieu.
2. Si les circonstances ne le permettent pas ou si le responsable ne donne pas suffisamment suite au signalement, la violation (présumée) de l'intégrité peut être signalée, selon le cas, à une personne de confiance locale.
3. Le lanceur d'alerte a également toujours le droit de consulter ses représentants du personnel ou les syndicats. Il continuera d'être protégé contre toute mesure défavorable injustifiée résultant de ces consultations.
4. Si le lanceur d'alerte estime qu'il ne peut pas s'adresser à ces personnes pour une raison quelconque, il peut faire un signalement interne.

Un signalement interne est un signalement d'un manquement au sein d'une entité juridique (l'entreprise) en fournissant des informations sur les manquements, oralement ou par écrit, par le biais du canal de signalement interne, dont la procédure est détaillée au titre "4.2. dépôt d'un signalement par le canal de signalement interne".

5. Après avoir utilisé la voie de communication interne, ou dans le cas exceptionnel où le lanceur d’alerte estimerait qu’il ne peut pas utiliser la voie de communication interne malgré les garanties prescrites par la présente politique (telles que la confidentialité, la protection contre les représailles et autres), il peut faire une communication externe, verbale ou écrite, par le biais de la voie de communication externe organisée par le gouvernement, comme expliqué plus en détail au titre "4.3. Soumettre un signalement par le biais du canal externe du gouvernement".
6. Le signalement public ou la divulgation publique d'informations sur les violations est possible si des conditions strictes sont remplies, comme indiqué au titre "4.4. Divulgation publique de la violation dans des circonstances exceptionnelles".

4.2. Soumettre un signalement par le biais du canal interne

Le lanceur d’alerte a la possibilité de soumettre un rapport anonyme. Un signalement anonyme peut toutefois présenter certains inconvénients :

- Le suivi du signalement est moins évident car la communication subséquente est plus difficile avec les lanceurs d’alerte anonymes ;
- Il est plus difficile pour l'entreprise de protéger un lanceur d’alerte anonyme contre des représailles éventuelles ou plutôt subtiles.

La soumission d'un signalement se fait oralement ou par écrit via

- E-mail : signalement@JGI.be ;
- Une rencontre physique dans un délai raisonnable.

Un signalement doit contenir au moins :

- Le nom, l'adresse, la fonction et les coordonnées du lanceur d’alerte s'il ne souhaite pas faire une déclaration anonyme ;
- La date du signalement ;
- Une description détaillée de la violation (présumée), telle que
 - La description de l'infraction (présumée) éventuellement avec des pièces jointes (documentation ou pièces justificatives) ;
 - L’identification des éventuelles personnes concernées ou des services de l'entreprise ;
 - Le lieu où la violation (présumée) s'est produite ;
 - Le moment où la violation (présumée) s'est produite ;
 - Comment et quand l’information de la violation (présumée) est intervenue ;
 - La relation du lanceur d’alerte avec l'entreprise (employé, free-lance, fournisseur, actionnaire, etc.) dans la mesure où la dénonciation n’est pas anonyme ;
 - L'impact de l'incident (pour l'entreprise, pour l'intérêt public, ...) ;
 - Toute autre information pertinente concernant la violation (présumée).



L'employeur a désigné un gestionnaire de signalement. C'est la personne ou le service le plus approprié au sein de l'organisation pour gérer les rapports de manière confidentielle et indépendante sans risque de conflit d'intérêts. En l'occurrence, pour JGI, il s'agit du Département des Ressources Humaines et du Département des Affaires réglementaires.

Recevabilité et enquête préliminaire

- a) Dans tous les cas, le gestionnaire de signalement confirme au lanceur d'alerte la réception du signalement effectué par écrit et ce dans les sept (7) jours à compter de cette réception.
 - Le gestionnaire de signalement examinera dans un premier temps si le signalement est admissible et procédera à une première évaluation à cet effet. L'objectif de celle-ci est essentiellement d'évaluer la nature, la fiabilité et l'exactitude des informations fournies.
 - En fonction de cette évaluation, le gestionnaire de signalement décidera si le signalement est recevable ou non et il devra alors informer le lanceur d'alerte par écrit du motif du rejet ou du lancement d'une enquête préliminaire concernant le fait rapporté.
- b) Si une enquête préliminaire est lancée et que le gestionnaire de signalement estime qu'une enquête plus approfondie s'impose, un avis anonyme peut ensuite être transmis avec l'accord du lanceur d'alerte à la Direction de site.

Cet avis doit reprendre les raisons pour lesquelles une telle enquête s'impose ainsi qu'une ébauche de plan d'action.
- c) Si l'enquête préliminaire révèle qu'il s'agit d'une fausse alerte intentionnelle, le dossier sera alors repris par le Directeur des Ressources Humaines afin que celui-ci prenne les mesures qui s'imposent.

Enquête

- a) Sur la base de l'avis précité, le Gestionnaire de signalement décidera si une enquête doit être menée et avec quel moyen ou support : experts internes ou externes, tierce partie externe, éventuellement assistée par des collaborateurs internes.
- b) Le lanceur d'alerte sera également informé par écrit du lancement d'une enquête plus approfondie.
- c) Le comité d'enquête mène son action dans un délai raisonnable. Tout doit être mis en œuvre afin que le délai ne dépasse pas trois mois à partir de l'envoi de l'accusé de réception au lanceur d'alerte. Dans ce délai, le lanceur d'alerte recevra également un retour d'information sur le suivi, l'action prévue ou entreprise, et les raisons de ce suivi.
- d) Au cours de l'enquête, des informations d'ordre général concernant la progression de l'enquête et les premières conclusions seront communiquées au lanceur d'alerte, sauf si ce dernier ne le souhaite pas ou si cela pourrait s'avérer préjudiciable pour celui-ci ou pour l'enquête, ou s'il existe d'autres raisons fondées de ne pas l'en informer.



Rapport final

Le rapport final comprend les étapes suivantes :

- a) Le comité d'enquête transmet ses conclusions par écrit au président du Comité, lequel décide des suites à apporter.
- b) Le gestionnaire de signalement informe le lanceur d'alerte que les conclusions du comité d'enquête ont été transmises au président du Comité.
- c) Dans le rapport final, l'identité du lanceur d'alerte est dissimulée, à moins que ce dernier n'ait consenti par écrit à ce que son identité soit révélée. L'identité de la ou des personne(s) mise(s) en cause n'est indiquée que si l'enquête menée suite au signalement a mis au jour des faits démontrables.
- d) Si le comité d'enquête estime que des sanctions doivent être prises, il transmettra une copie du rapport final à la personne compétente au sein de la direction.

4.3. Soumettre un rapport par le biais du canal externe du gouvernement

Après avoir effectué un premier signalement par le biais d'un canal interne, le lanceur d'alerte (anonyme) peut signaler une violation par le biais d'un canal gouvernemental externe si aucune mesure appropriée n'a été prise par le biais de la procédure interne. Le lanceur d'alerte peut également faire immédiatement un signalement par le biais du canal de signalement externe du gouvernement.

Le canal de signalement externe permet des signalements écrits et oraux auprès du Médiateur Fédéral. Le signalement oral est possible par téléphone ou autre système de messagerie vocale et à la demande du lanceur d'alerte, par une rencontre physique dans un délai raisonnable. Le canal d'information externe du gouvernement est accessible par le Médiateur Fédéral :

- E-mail : integrite@mediateurfederal.be
- Tél. : 02/289.27.04
- Formulaire de signalement en ligne : <https://www.federaalombudsman.be/fr/formulairesignalement>

Le canal de signalement externe indépendant enverra un accusé de réception dans les sept (7) jours, sauf si :

- Le lanceur d'alerte indique explicitement qu'il ne veut pas cet accusé de réception
- L'accusé de réception peut constituer une menace pour la protection de l'identité du lanceur d'alerte.

Le canal de signalement externe fournira un retour d'information dans un délai de trois mois, ou dans des cas particuliers (notamment lorsque les enquêtes à mener s'avèrent longues), de six mois, au lanceur d'alerte du suivi prévu ou des mesures prises et des raisons de ce suivi, à moins qu'une disposition légale ne l'empêche. Le canal de signalement externe informera le lanceur d'alerte du résultat final des investigations.



Les autorités compétentes peuvent décider qu'une infraction signalée est manifestement d'importance mineure ou a déjà fait l'objet de notifications antérieures portant sur les mêmes faits sans éléments nouveaux supplémentaires, ce qui a pour effet de clore la procédure. Les autorités compétentes informent le lanceur d'alerte de leur décision et des raisons qui la motivent.

4.4. Divulqation publique d'une violation dans des circonstances exceptionnelles

Un lanceur d'alerte (anonyme) qui divulgue une violation en rendant publiques des informations sur les violations (par exemple par le biais des médias) peut bénéficier d'une protection si les conditions suivantes sont remplies :

- Le lanceur d'alerte a d'abord fait un rapport interne ou externe comme prescrit aux titres 4.2 ou 4.3 mais aucune mesure appropriée n'a été prise ;
- Et le lanceur d'alerte a des motifs raisonnables de croire que :
 - La violation peut représenter un danger imminent ou réel pour l'intérêt public ; ou
 - Dans le cas d'un signalement externe, il existe un risque de représailles, ou il est peu probable qu'il soit véritablement remédié à la violation, en raison des circonstances particulières de l'affaire, parce que, par exemple, les preuves peuvent être dissimulées ou détruites, ou une autorité peut être en collusion avec l'auteur de la violation ou être impliquée dans la violation.

5. Garanties pour le statut du lanceur d'alerte

5.1. Conditions de protection

Les lanceurs d'alertes sont protégés si :

- Ils ont des motifs raisonnables de croire que les informations communiquées sur les violations au moment du signalement étaient véridiques et qu'elles entraient dans le cadre de cette politique. Le lanceur d'alerte ne perd pas le bénéfice de la protection au seul motif que la déclaration faite de bonne foi s'est révélée fausse ou infondée ; et
- Ils rapportent l'information par le biais du canal de rapport interne ou externe. Le lanceur d'alerte bénéficie également d'une protection s'il divulgue publiquement la violation dans la mesure où il a d'abord fait un rapport interne ou externe.

Les lanceurs d'alerte anonymes qui ont signalé ou divulgué des informations sur des violations mais qui ont été identifiés par la suite et ont fait l'objet de représailles peuvent bénéficier d'une protection s'ils remplissent ces conditions.

Les personnes physiques et morales suivantes bénéficient d'une protection si elles ont des motifs raisonnables de croire que le lanceur d'alerte relève de la condition de protection :

- Les facilitateurs ;
- Les tiers liés aux lanceurs d'alerte qui risquent d'être victimes de représailles dans un contexte professionnel, tels que les collègues ou les membres de la famille des lanceurs d'alerte ;
- Les entités juridiques appartenant aux lanceurs d'alerte, pour lesquelles ils travaillent ou avec lesquelles ils sont autrement liés dans un contexte professionnel.



5.2. Confidentialité

Le gestionnaire de signalement, y compris le personnel autorisé chargé de la réception et du suivi des signalements, doit garder confidentielle l'identité du lanceur d'alerte. Le gestionnaire de signalement est également désigné en raison des qualités de confidentialité du dossier, de l'identité du lanceur d'alerte et de l'indépendance du service pour éviter les conflits d'intérêts. Plus particulièrement, une interdiction de communiquer l'identité du lanceur d'alerte – ou des éléments permettant d'identifier celui-ci – s'applique pendant la durée du traitement, sauf si la personne concernée a donné son consentement à cet effet. L'obligation de confidentialité s'applique également si un lanceur d'alerte anonyme devient directement ou indirectement identifiable par d'autres informations.

Le gestionnaire de signalement ne peut divulguer l'identité du lanceur d'alerte que :

- Si le lanceur d'alerte en donne l'autorisation libre et expresse (par écrit) ; ou
- Si le lanceur d'alerte lui-même rompt délibérément la confidentialité.

La confidentialité de l'identité ne s'appliquera pas si une législation impérative exige la divulgation dans le cadre d'enquêtes menées par les autorités nationales ou de procédures judiciaires. L'autorité compétente informera à l'avance les lanceurs d'alerte des raisons de la divulgation, à moins que cela ne compromette des enquêtes ou des procédures judiciaires.

Toute personne impliquée directement ou indirectement dans le traitement d'un signalement d'une violation (présumée) de l'intégrité est tenue au secret professionnel concernant toutes les informations qui lui sont communiquées (le signalement, l'enquête préliminaire et l'enquête proprement dite) ou dont elle prend connaissance, et ce vis-à-vis de toute personne ne pouvant avoir accès à ces informations, pour autant que ces obligations découlent de la nature de l'affaire.

Le canal interne de réception des signalements est tenu, par sa conception, sa mise en place et sa gestion, de protéger de manière sûre la confidentialité de l'identité du lanceur d'alerte et de tout tiers nommé dans le signalement et auquel le personnel non autorisé ne peut avoir accès.

5.3. Prévenir les représailles, telles que les sanctions ou les traitements injustes.

Une mesure de représailles est un acte ou une omission directe ou indirecte qui se produit dans un contexte professionnel au détriment d'un lanceur d'alerte en réponse à un signalement ou une divulgation interne ou externe, et qui entraîne ou peut entraîner un préjudice injustifié pour le lanceur d'alerte.



Toute forme de représailles, y compris les menaces et les tentatives de représailles, est interdite et concerne spécifiquement :

- Suspension, mise à pied, licenciement ou mesures similaires ;
- Rétrogradation ou refus de promotion ;
- Transfert de fonctions, changement de lieu de travail, réduction de salaire, modification des horaires de travail ;
- Suspension de la formation ;
- Une évaluation de performance ou attestation de travail négative ;
- Imposer ou appliquer une mesure disciplinaire, une réprimande ou une autre sanction, telle qu'une sanction financière ;
- La coercition, l'intimidation, le harcèlement ou l'exclusion ;
- Une discrimination, traitement défavorable ou injuste ;
- La non-conversion d'un contrat de travail temporaire en un contrat de travail à durée indéterminée, dans le cas où le salarié s'attendait légitimement sur base d'évaluation objective des compétences à ce qu'on lui propose un emploi à durée indéterminée ;
- Le non-renouvellement ou la résiliation anticipée d'un contrat de travail temporaire ;
- Des dommages, notamment en termes de réputation, en particulier sur les médias sociaux, ou des pertes financières, y compris des pertes de ventes et de revenus ;
- Une mise sur liste noire basée sur un accord informel ou formel pour tout un secteur ou une industrie, qui empêche la personne de trouver un emploi dans ce secteur ou cette industrie ;
- La résiliation ou l'annulation anticipée d'un contrat de fourniture de biens ou de services ;
- La révocation d'une licence ou d'un permis.

Les lanceurs d'alerte qui agissent conformément à ce système peuvent signaler une violation (présumée) sans mettre en péril leur statut au regard du droit du travail. Ceci implique qu'ils ne peuvent en aucun cas être traités de manière moins favorable en raison de la question posée ou du signalement effectué, et ce pour autant qu'ils aient agi de bonne foi.

Toutes représailles à l'encontre d'un lanceur d'alerte à la suite d'une alerte justifiée seront considérées comme une violation grave de ce système d'alerte professionnelle ainsi que du code de conduite de l'employeur, en conséquence de quoi des mesures appropriées seront prises pour protéger le statut du lanceur d'alerte et sanctionner les responsables de ces représailles.

Les collaborateurs qui estiment avoir été traités injustement après avoir effectué un signalement sont priés d'en avvertir le plus rapidement possible le gestionnaire des signalements. Il conviendra à chaque fois de pouvoir démontrer un lien de causalité entre le signalement et la mesure de représailles dénoncée.

La victime de représailles peut également déposer une plainte motivée auprès du coordinateur fédéral, qui engagera une procédure de protection extrajudiciaire s'il a établi une suspicion raisonnable de représailles. Le coordinateur fédéral qui traitera cette plainte est le Médiateur Fédéral dont les coordonnées figurent à l'article "4.3 *Soumettre un rapport par l'intermédiaire du canal de signalement externe du gouvernement*".



Le coordinateur fédéral vérifie auprès de l'employeur l'existence d'une suspicion raisonnable de représailles. L'employeur répondra à la demande du coordinateur fédéral dans les 20 jours.

5.4. Utilisation abusive du système d'alerte professionnelle

L'employeur part du principe que les lanceurs d'alerte exprimeront leurs préoccupations de bonne foi. Si l'enquête ne permet pas de confirmer le signalement en question ou si celui-ci s'avère non fondé, aucune mesure ne sera prise contre le lanceur d'alerte qui a fait part de ses préoccupations de bonne foi.

En revanche, l'employeur ne peut tolérer que des signalements, dont le caractère non fondé est connu ou est supposé être connu, ne soient effectués de manière intentionnelle. L'employeur sanctionnera de manière appropriée les déclarations délibérément fausses selon les sanctions prévues par la réglementation du travail. Le lanceur d'alerte de mauvaise foi peut être tenu responsable des dommages subis par les personnes à la suite de faux rapports.

Le lanceur d'alerte qui a délibérément rapporté ou divulgué de fausses informations peut faire l'objet de poursuites pénales pour atteinte à l'honneur ou à la réputation des personnes.

6. Le traitement des données à caractère personnel et vos droits

L'employeur est responsable du traitement des données à caractère personnel dans le cadre de l'exécution de ce système d'alerte professionnelle. Cela implique que tant le lanceur d'alerte que la personne concernée peuvent s'adresser à l'employeur pour exercer leurs droits d'information, d'accès, de rectification, de portabilité et de suppression des données, en tenant compte des limitations suivantes :

- La personne mise en cause ne peut accéder à l'identité du lanceur d'alerte ou à celle de tiers (ou à des éléments qui permettraient leur identification), sauf s'ils ont donné leur accord en ce sens, ou en cas de fausse alerte ou d'accusations calomnieuses du lanceur d'alerte ou de faux témoignage d'un tiers ;
- Le lanceur d'alerte n'a pas non plus le droit d'accéder aux données à caractère personnel de la personne mise en cause, ni à celles de tiers. Cette interdiction d'accès peut toutefois être levée lorsque, après enquête, il apparaît que la personne mise en cause a suspecté à tort le lanceur d'alerte (en affirmant par exemple que ce dernier était lui-même impliqué dans les pratiques abusives) ou si des tiers ont agi de mauvaise foi (par exemple en faisant de faux témoignages) ;
- Les données à caractère personnel des parties concernées ne seront pas supprimées tant que l'enquête interne et/ou externe (policière/judiciaire/administrative) sera en cours.

Les données à caractère personnel ne seront pas transférées vers des pays tiers n'offrant pas un niveau de protection adéquat de vos données à caractère personnel.



Durant la procédure de signalement, outre les faits, le nom, la fonction et les coordonnées du lanceur d'alerte et de la personne mise en cause seront traités. Le traitement de ces données à caractère personnel est nécessaire en vertu de la loi du 28 novembre 2022 relative à la protection des auteurs d'infractions au droit de l'Union ou au droit national établis au sein d'une personne morale du secteur privé (art. 6, §1, c) RGPD). Le transfert d'une notification à un sous-traitant (prestataire de services tel qu'un fournisseur de stockage de datas) peut être effectué sur la base des intérêts légitimes de l'employeur à traiter efficacement ces données aux fins de la gestion des notifications, de la garantie de l'anonymat, de la gestion des accès, etc. (Article 6, §1, f) RGPD).

Si, après avoir pris contact avec l'employeur, vous souhaitez tout de même introduire une plainte concernant le traitement de vos données à caractère personnel, vous pouvez vous adresser à l'autorité de contrôle compétente, à savoir l'Autorité de Protection des Données.

L'autorité en charge du canal de communication externe agit en tant que responsable du traitement des données. Cela signifie qu'en cas de signalements externes, vous pouvez vous adresser au gouvernement pour faire valoir vos droits.

Les autorités compétentes et l'Institut fédéral pour la protection et la promotion des droits de l'homme (accessible via ce [lien](https://institutfederaldroitshumains.be/fr/vous-avez-des-questions-contactez-nous) : <https://institutfederaldroitshumains.be/fr/vous-avez-des-questions-contactez-nous> ou via info@firm-ifdh.be) vous informeront et vous conseilleront sur les mesures de soutien, telles que :

- Des informations et des conseils sur les recours et les procédures disponibles qui protègent contre les représailles, ainsi que sur les droits de la personne concernée ;
- Des conseils techniques envers les autorités impliquées dans la protection du lanceur d'alerte ;
- Aide juridique et assistance financière dans les procédures judiciaires ;
- Soutien technique, psychologique, médiatique et social.

7. Délai de conservation

Les données à caractère personnel traitées dans le cadre de ce système d'alerte professionnelle ne seront pas conservées plus longtemps que nécessaire aux fins de l'enquête interne et/ou externe (policière/judiciaire/administrative). En cas de procédure judiciaire ou disciplinaire, une fois la procédure terminée ou après expiration du délai de recours applicable, les données seront archivées ou conservées pendant six mois maximum.



8. Sanctions

Les infractions énumérées, entre autres au point « 3. *Champ d'application* » de la présente politique relative au système d'alerte professionnelle et constatées lors de l'enquête menée à la suite d'une alerte lancée par le biais de ce système d'alerte professionnelle, peuvent donner lieu à des sanctions (notamment avertissement ou licenciement pour motif grave) telles que décrites dans le règlement de travail ou dans le contrat de travail.

Outre ces sanctions relevant du droit du travail, en fonction de la nature de la violation et du droit applicable, la personne concernée ou le lanceur d'alerte de mauvaise foi peuvent encourir des sanctions supplémentaires, telles que des sanctions pénales et des dommages et intérêts.

9. Collaboration de la direction

En vue d'un bon ancrage de ce système d'alerte professionnelle au sein de l'organisation, la direction :

- Veillera à ce que ce système soit facilement accessible et connu de l'ensemble des collaborateurs ;
- Prendra au sérieux tous les signalements de violations de l'intégrité, interviendra en temps opportun, garantira le respect de la confidentialité et fera preuve de la diligence requise.

10. Autres provisions

Ce régime sera réexaminé dans les deux ans suivant son entrée en vigueur.

Pour les cas non prévus dans ce système, la décision reviendra au président du Comité d'audit.

Fait à Bruxelles

Date : 01/01/2025

Bernard Moonen
Directeur des Ressources Humaines

Philippe Henry
Directeur Général