

POLITIQUE RELATIVE AUX LANCEURS D'ALERTE CLAES RETAIL GROUP SA

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, est une transposition de la Directive européenne 2019/1937 sur la protection des personnes qui signalent des violations du droit de l'Union. La loi protège les travailleurs et les tiers qui souhaitent signaler une violation au droit de l'Union constatée au sein d'une entité juridique du secteur privé.

La présente politique relative aux lanceurs d'alerte a pour but d'apporter aux collaborateurs de CLAES RETAIL GROUP SA¹, ainsi qu'à certaines parties prenantes, une transparence à propos des canaux disponibles pour signaler de telles irrégularités (présumées) au sein de C.R.G..

C.R.G. souhaite ainsi lutter contre les éventuelles pratiques ou actes illégaux, frauduleux ou interdits à d'autres titres qui tombent sous le contrôle de l'entreprise ou une de ses filiales, à garantir une enquête indépendante et confidentielle et à éviter les éventuels conflits d'intérêts. La présente politique n'implique toutefois aucune obligation de signalement, mais représente uniquement une opportunité pour les collaborateurs de C.R.G. et des tiers de signaler des irrégularités au sein de l'entreprise, sous couvert de certaines garanties.

1. Définitions

Les définitions suivantes s'appliquent à la présente politique :

- « **informations sur des violations** » : des informations, y compris des soupçons raisonnables, concernant des violations effectives ou potentielles, qui se sont produites ou sont très susceptibles de se produire, et concernant des tentatives de dissimulation de telles violations;
- « **signalement** » ou « **signaler** » : la communication orale, écrite ou électronique d'informations sur des violations ;
- « **signalement interne** » : la communication orale ou écrite d'informations sur des violations au sein d'une entité juridique du secteur privé ;
- « **signalement externe** » : la communication orale ou écrite d'informations sur des violations au coordinateur fédéral ou aux autorités compétentes ;
- « **divulgaration** » ou « **divulguer publiquement** » : la mise à disposition dans la sphère publique d'informations sur des violations;
- « **auteur de signalement** » ou « **lanceur d'alerte** » : une personne qui signale ou divulgue publiquement des informations sur des violations ;
- « **contexte professionnel** » : activités professionnelles passées ou présentes dans le secteur privé par lesquelles, indépendamment de la nature de ces activités, des personnes obtiennent des informations sur des violations dans le cadre desquelles ces personnes pourraient faire l'objet de représailles;
- « **facilitateur** » : une personne physique qui aide un auteur de signalement au cours du processus de

¹ CLAES RETAIL GROUP SA, est le holding qui chapeaute les marques de mode JBC, CKS et Mayerline.

Cette politique s'applique aux entités juridiques suivantes :

- C.R.G. NV, dont le siège social est situé Centrum Zuid 3401, 3530 Houthalen, KBO 0462.417.806
- JBC NV, dont le siège social est situé Centrum Zuid 3401, 3530 Houthalen, KBO 0429.340.608
- Mayerline NV, dont le siège social est situé Centrum Zuid 3401, 3530 Houthalen, KBO 0400.573.277.

- signalement dans un contexte professionnel et dont l'aide devrait être confidentielle;
- « **personne concernée** » : 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;
 - « **représailles** » : tout acte ou omission direct ou indirect qui intervient dans un contexte professionnel, est suscité par un signalement interne ou externe ou une divulgation publique, et qui cause ou peut causer un préjudice injustifié à l'auteur de signalement;

2. Champ d'application personnel :

La présente politique s'applique aux lanceurs d'alerte ayant été informés de violations dans un contexte professionnel. Cela signifie que les canaux de signalement et mécanismes de protection repris ci-dessous sont accessibles aux personnes suivantes, entre autres :

1. Les travailleurs actuels de C.R.G. ;
2. Les ex-travailleurs si des informations sur des violations ont été obtenues dans le cadre d'une relation professionnelle entre-temps terminée ;
3. Les candidats-collaborateurs si des informations sur des violations ont été obtenues dans le cadre de la procédure d'embauche ou autres négociations précontractuelles ;
4. Les prestataires de services indépendants au sein de C.R.G. (tels que les freelances, les consultants) ;
5. Les actionnaires et les personnes membres de l'organe d'administration, de direction ou de contrôle de C.R.G., en ce compris les membres, bénévoles et stagiaires rémunérés ou non qui ne sont pas impliqués dans la gestion journalière ;
6. Toute personne qui travaille sous la supervision et la direction d'entrepreneurs, sous-traitants et fournisseurs.
7. Les facilitateurs ;
8. Les tiers qui sont liés aux lanceurs d'alerte et susceptibles d'être victimes de représailles dans un contexte professionnel, tels que les collègues ou les proches des lanceurs d'alerte ;
9. Les entités juridiques qui appartiennent aux auteurs de signalement, pour lesquelles ceux-ci travaillent ou auxquelles ils sont autrement liés dans un contexte professionnel.

3. Champ d'application matériel :

Les canaux de signalement peuvent être utilisés pour dénoncer les violations suivantes :

- 1° Violations qui portent sur les domaines suivants :
 - a) marchés publics ;
 - b) services, produits et marchés financiers, prévention du blanchiment de capitaux et du financement du terrorisme ;
 - c) sécurité et conformité des produits ;
 - d) sécurité des transports ;
 - e) protection de l'environnement ;
 - f) radioprotection et sûreté nucléaire ;
 - g) sécurité des aliments destinés à l'alimentation humaine et animale, santé et bien-être des animaux ;
 - h) santé publique ;
 - i) protection des consommateurs ;

- j) protection de la vie privée et des données à caractère personnel, et sécurité des réseaux et des systèmes d'information ;
 - k) lutte contre la fraude fiscale ;
 - l) lutte contre la fraude sociale.
- 2° Violations (comme la fraude, par exemple) portant atteinte aux intérêts financiers de l'Union européenne (cfr. article 325 du Traité sur le fonctionnement de l'Union européenne) ;
- 3° Violations des règles de l'Union en matière de concurrence et d'aides d'État et autres violations relatives au marché intérieur (cfr. Article 26, alinéa 2, du Traité sur le fonctionnement de l'Union européenne).
- 4° Tentatives de dissimulation d'informations liées à un des éléments ci-dessus.

Ne relèvent toutefois **pas** du champ d'application de la présente politique relative aux lanceurs d'alerte :

- Les plaintes pour violences, harcèlement moral et sexuel, que le travailleur qui s'estime victime de tels actes peut soumettre à la personne de confiance désignée à cet effet dans le règlement de travail ou au conseiller en prévention aspects psychosociaux du service externe de prévention et de protection au travail.
- Les signalements relatifs à des informations classifiées ;
- Les signalements sur la base d'informations couvertes par le secret médical ;
- Les signalements sur la base d'informations couvertes par le secret des délibérations judiciaires.
- Les plaintes relatives à la prestation de services de C.R.G. (comme les plaintes relatives à des paiements de factures, par exemple).

Lorsqu'il effectue un signalement, le lanceur d'alerte doit toujours agir de bonne foi. Le signalement doit être fondé sur des motifs raisonnables. Lorsque le signalement contient des allégations fausses, infondées ou opportunistes, ou s'il est fait dans un but inapproprié, tel que diffamer ou causer un préjudice à autrui, C.R.G. peut ignorer le signalement et, le cas échéant, prendre des mesures appropriées.

4. Procédures de signalement

Il existe trois façons d'effectuer un signalement :

- Signalement interne
- Signalement externe
- Divulgarion publique

Si vous constatez, prenez connaissance ou soupçonnez raisonnablement une violation (potentielle) qui survient ou est survenue au sein de C.R.G., il vous est conseillé de le signaler en interne dans un premier temps.

4.1. Procédure de signalement interne

Un auteur de signalement, tel que décrit sous 'Champ d'application personnel', qui estime qu'il existe une irrégularité, telle que décrite dans 'Champ d'application matériel', peut effectuer un signalement auprès du gestionnaire des plaintes désigné à cet effet. Un signalement s'effectue de préférence par courrier électronique

ou postal, mais également verbalement, sur rendez-vous de préférence, par téléphone ou, si l'auteur du signalement en fait la demande, au moyen d'une rencontre en personne organisée dans un délai raisonnable.

Est désignée en tant que gestionnaire des plaintes de C.R.G. :

Annick Thijs

Centrum Zuid 3401

3530 Houthalen

E.: blowthewhistle@claesretailgroup.com (+32 11 60 84 00)

Le gestionnaire des plaintes qui reçoit un signalement transmet au lanceur d'alerte un accusé de réception du signalement dans les 7 jours ouvrables qui suivent sa réception.

Le gestionnaire des plaintes enregistre le signalement avec la date de réception et il est la seule personne à connaître l'identité du lanceur d'alerte. La confidentialité de l'identité du lanceur d'alerte et de tout tiers éventuel nommé dans le signalement est garantie à tout moment. Les membres du personnel non autorisés n'ont pas accès au canal de signalement interne. En cas d'ambiguïtés dans le signalement initial, le gestionnaire des plaintes demande des précisions.

Le gestionnaire des plaintes est responsable du suivi diligent de chaque signalement (voir Incident Response Plan) :

Incident response plan

1. Après réception du signalement, le gestionnaire des plaintes convoque un comité interne. Le comité interne est constitué des membres de la direction des départements suivants : juridique – IT – HR - finance.
Si le signalement concerne de possibles violations au sein d'un des départements du comité interne, le département en question sera écarté du premier examen du signalement. Le gestionnaire des plaintes informera le comité interne de la plainte de manière confidentielle et anonyme.
2. Le comité interne définit les mesures d'enquête nécessaires en fonction des irrégularités présumées, comme par exemple, mis sans s'y limiter :
 - L'audition de l'auteur du signalement par le gestionnaire des plaintes concernant les irrégularités présumées.
 - L'audition de la personne ou des personnes qui, selon le signalement, est/sont impliquée(s) dans les irrégularités signalées.
 - La collecte d'informations et la consultation de sources nécessaires à la vérification des irrégularités alléguées, signalées par le lanceur d'alerte.
3. Le comité interne étudie l'impact que le signalement peut avoir sur la gestion, la réputation,... de l'entreprise.
4. Le comité interne rapporte ses constatations oralement et par écrit au comité de gestion journalière (la « direction ») de C.R.G..

5. Le comité de gestion journalière de C.R.G. prend une décision et des mesures éventuelles sur la base du rapport du gestionnaire des plaintes. Si le signalement porte sur un membre du conseil de gestion journalière, le rapport est adressé aux administrateurs délégués de C.R.G..
6. Le lanceur d'alerte et la ou les personnes incriminées sont informées de la clôture de l'enquête.

Lors de l'information et du signalement, le gestionnaire de signalement ne divulgue ni l'identité du lanceur d'alerte ni celle des tiers éventuels cités dans le signalement.

Le gestionnaire des plaintes fournit au lanceur d'alerte les informations relatives aux mesures prévues ou prises à titre de suivi et aux motifs de ce suivi, et ce dans les meilleurs délais, et au plus tard 3 mois après l'accusé de réception du signalement ou, à défaut d'accusé de réception envoyé au lanceur d'alerte, trois mois après l'expiration du délai de sept jours suivant le signalement.

Protection

1. Le traitement d'un signalement s'effectue en toute confidentialité.
2. Le comité de la gestion journalière de C.R.G. déclare qu'un signalement fait par un collaborateur au gestionnaire des plaintes sur la base du présent règlement relatif aux lanceurs d'alerte, ne peut avoir une influence négative sur le fonctionnement ou les opportunités de carrière de ce collaborateur au sein de l'entreprise.
3. Le lanceur d'alerte est prié de garder son signalement confidentiel et de ne pas le divulguer publiquement, que ce soit directement ou par l'intermédiaire de tiers, jusqu'à ce que le comité de gestion journalière de C.R.G. ait annoncé, par le biais du gestionnaire des plaintes, la fin de l'enquête.
4. Un lanceur d'alerte qui a volontairement effectué un signalement manifestement infondé, et a donc fait illégitimement usage de la procédure de signalement prévue dans le présent règlement sur les lanceurs d'alerte, peut être sanctionné à ce titre (voir ci-dessous).

Enregistrement de signalements

C.R.G. tient un registre de tous les signalements reçus, dans le respect des exigences de confidentialité applicables. Les signalements sont conservés pendant la durée de la relation contractuelle.

Lorsqu'une ligne téléphonique non enregistrée ou un autre système de messagerie non enregistré est utilisé pour le signalement, l'entreprise se réserve le droit d'enregistrer le signalement oral sous la forme d'un compte rendu circonstancié de la conversation, rédigé par le membre du personnel responsable du traitement du signalement. Le lanceur d'alerte a toujours la possibilité de contrôler, corriger et signer pour accord le compte rendu de la conversation.

Si une personne demande un entretien avec le gestionnaire des plaintes afin d'effectuer un signalement interne, C.R.G. veille, si le lanceur d'alerte y consent, à ce qu'un compte rendu complet et circonstancié de l'entretien soit consigné sous une forme durable et récupérable. C.R.G. se réserve le droit d'enregistrer le signalement oral de la manière suivante :

- par un enregistrement de la conversation sous une forme durable et récupérable ; ou
- par un compte rendu précis de l'entretien, établi par le membre du personnel chargé de traiter le signalement. Le lanceur d'alerte a toujours la possibilité de vérifier, corriger et signer pour accord le

compte rendu de l'entretien.

Droit à la protection de la vie privée

Les données à caractère personnel du lanceur d'alerte et de la ou des personnes incriminées, sont traitées de manière confidentielle et uniquement en vue du traitement d'un signalement et de l'enquête subséquente, conformément à la notification vie privée. Les personnes concernées peuvent invoquer, chacune individuellement, le droit de consultation et de correction des données traitées portant sur sa personne, conformément au Règlement Général sur la Protection des Données 2016/679 et la notification vie privée. Elles peuvent également s'adresser à cet effet à l'Autorité de protection des données. Elles n'ont pas accès aux données de tiers.

Politique de confidentialité pour les signalements internes

En utilisant les canaux de signalement interne repris dans la présente Politique relative aux lanceurs d'alerte, vous acceptez le traitement de vos données à caractère personnel aux finalités indiquées dans la présente Politique de lanceurs d'alerte.

a) Traitement des données à caractère personnel

Dans le cadre de sa « Politique relative aux lanceurs d'alerte », C.R.G. traitera des données à caractère personnel (1) de l'auteur du signalement et (2) de la personne concernée (c'est-à-dire la personne incriminée) en sa qualité de responsable du traitement.

Concrètement, C.R.G. traitera les données à caractère personnel suivantes qui sont liées à la plainte du lanceur d'alerte :

- données d'identification et de contact du lanceur d'alerte (nom/prénom/e-mail/numéro de téléphone) et des éventuelles autres personnes concernées ;
- (éventuel) enregistrement du signalement ;
- relation du lanceur d'alerte vis-à-vis de C.R.G. ;
- le contenu de la plainte ; et
- les données (à caractère personnel) liées à la plainte (notamment la personne incriminée et les preuves).

C.R.G. ne traite pas de catégories particulières² de données à caractère personnel du lanceur d'alerte, sauf si cela devait s'avérer strictement nécessaire dans le cadre du traitement de la plainte. En cas de collecte de catégories particulières de données à caractère personnel par C.R.G. dans le cadre de la « Politique relative aux lanceurs d'alerte », ces données à caractère personnel seront alors traitées avec la sécurité nécessaire et conformément à la base juridique appropriée.

C.R.G. traite toujours les données à caractère personnel susmentionnées conformément à la législation européenne et nationale en vigueur en matière de respect de la vie privée, ce qui inclut, sans s'y limiter (1) le Règlement général sur la protection des données (UE) 2016/679 (ci-après « **RGPD** ») et (2) la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

² Les catégories particulières de données à caractère personnel incluent l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions, l'appartenance syndicale, et le traitement de données génétiques, données biométriques, concernant la santé, ou des données concernant la vie sexuelle et l'orientation sexuelle.

b) Finalités du traitement

C.R.G. traite en outre les données à caractère personnel susmentionnées de manière confidentielle et uniquement en vue de la mise à exécution de la « Politique relative aux lanceurs d’alerte » qui découle du respect d’obligations légales. Pour toute question concernant le traitement de vos données à caractère personnel, veuillez nous contacter par courriel à l’adresse électronique legal@jbc.be.

Concrètement, C.R.G. traite ces données à caractère personnel afin de respecter les finalités qui découlent de la législation précitée et de sa « Politique relative aux lanceurs d’alerte », et afin de pouvoir traiter la plainte du lanceur d’alerte, l’apprécier et l’examiner plus avant lorsque cela est nécessaire, ainsi que pour pouvoir éventuellement se défendre dans le cadre de procédures judiciaires (les données à caractère personnel sont traitées sur pied de l’article 6.1 (c) et (f) RGPD « nécessaire au respect d’une obligation légale » et « intérêts légitimes »).

c) Transmission

Les données à caractère personnel collectées dans le cadre de la présente Politique relative aux lanceurs d’alerte peuvent être partagées avec des travailleurs (dirigeants) dûment désignés de C.R.G., ainsi qu’avec des prestataires de services qui défendent les intérêts de C.R.G., si cela s’avère nécessaire pour assurer le suivi du signalement. Le paragraphe 4.1 de la présente Politique relative aux lanceurs d’alerte indique quel travailleur a accès aux données à caractère personnel, quand et pour quelle raison.

Si nous y sommes légalement tenus, vos données à caractère personnel pourront être transmises aux autorités de surveillance, aux autorités fiscales et aux services d’enquête.

d) Sécurité

C.R.G. a mis en place des mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel reçues et garantir les finalités de la « Politique relative aux lanceurs d’alerte ». Concrètement, C.R.G. a mis en œuvre des normes de sécurité qui protègent les données à caractère personnel contre la perte, l’usage abusif, la modification et l’accès non autorisé.

e) Délai de conservation

Les données à caractère personnel seront conservées aussi longtemps que nécessaire pour le traitement et la gestion du signalement, en ce compris les mesures éventuelles et le suivi de celles-ci. Les données peuvent être conservées plus longtemps si et dans la mesure où cela est nécessaire dans le cadre d’une procédure judiciaire.

f) Droits

Le lanceur d’alerte a le droit, sous certaines conditions :

- d’avoir accès à ses données à caractère personnel ;
- de corriger ses données à caractère personnel ;
- de supprimer ses données à caractère personnel ;
- de limiter le traitement de ses données à caractère personnel ;
- le droit de s’opposer au traitement de ses données à caractère personnel ;

- le droit à la portabilité de ses données à caractère personnel ;
- le droit de demander la transmission de ses données à caractère personnel et
- le droit de retirer à tout moment son consentement (le cas échéant).

Le lanceur d’alerte peut exercer les droits précités en contactant legal@jbc.be et en remettant les pièces justificatives nécessaires à C.R.G.. Veuillez noter qu’à la suite de l’exercice de certains des droits précités, il est possible que C.R.G. ne puisse pas respecter ses obligations en vertu de la « Politique relative aux lanceurs d’alerte » et/ou de la législation applicable, auquel cas C.R.G. avisera le lanceur d’alerte que l’exercice des droits susmentionnés n’est pas possible en raison de la réglementation actuellement en vigueur. C.R.G. fournira tous les efforts raisonnables et pratiques pour satisfaire la demande, à condition que celle-ci soit conforme à la législation applicable et aux normes professionnelles.

g) Plaintes

Le lanceur d’alerte a la possibilité d’introduire une plainte auprès de l’Autorité belge de protection des données s’il estime que le traitement de ses données à caractère personnel est contraire au RGPD (<https://www.autoriteprotectiondonnees.be/contact>). Ensuite, le lanceur d’alerte a toujours la possibilité de contacter C.R.G. à l’adresse privacy@jbc.be.

4.2. Procédure de signalement externe

Un lanceur d’alerte a la possibilité de signaler des violations par le biais de canaux et procédures de signalement externe après avoir dans un premier temps effectué un signalement par le biais des canaux de signalement interne ou par un signalement direct par l’intermédiaire des autorités compétentes.

Il est hautement recommandé de d’abord signaler les violations (présumées) en interne. Les signalements internes restent les plus efficaces pour permettre à C.R.G. de mener une enquête approfondie sur la question et de prendre les mesures appropriées pour remédier à la mauvaise conduite.

Autorités compétentes

Les autorités compétentes pour recevoir des signalements, fournir un retour d’information et assurer le suivi des signalements, sont les suivantes :

1. le Service public fédéral Économie, P.M.E., Classes moyennes et Énergie ;
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 fédéral de Programmation Intégration Sociale, Lutte contre la pauvreté, Économie 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 de la fourniture et de 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 ;
22. le Service d'information et de recherche sociale ;
23. le Service autonome de Coordination Anti-Fraude (CAF) ;
24. le Contrôle de la navigation.

En l'absence de désignation ou si aucune autorité ne s'estime compétente pour recevoir un signalement, le Médiateur fédéral agit en qualité d'autorité compétente pour recevoir les signalements, fournir un retour d'informations et assurer le suivi des signalements.

Procédure de signalement externe

Un lanceur d'alerte qui estime qu'une violation a été commise peut effectuer un signalement auprès de l'autorité compétente ou du Médiateur fédéral.

Chaque autorité doit avoir établi un canal de signalement externe indépendant et autonome pour la réception et le traitement des informations sur des violations. Les canaux de signalement externe permettent d'effectuer des signalements par écrit et oralement. Il est possible d'effectuer des signalements oralement par téléphone ou via d'autres systèmes de messagerie vocale et, sur demande du lanceur d'alerte, par le biais d'une rencontre en personne dans un délai raisonnable.

Les autorités compétentes désignées précisent, par voie de règlement ou de circulaire, les règles de procédure concrètes applicables à la réception et au traitement des signalements.

L'autorité compétente est tenue d'accuser réception des signalements dans un délai de sept jours à compter de la réception du signalement, sauf demande contraire expresse du lanceur d'alerte ou à moins que l'autorité compétente ait des motifs raisonnables de croire qu'accuser réception du signalement compromettrait la protection de l'identité du lanceur d'alerte.

L'autorité compétente assure un suivi diligent des signalements, en ce compris des signalements anonymes, et fournit au lanceur d'alerte un retour d'informations dans un délai raisonnable n'excédant pas trois mois, ou six mois dans des cas dûment justifiés, sauf lorsqu'une disposition légale l'en empêche.

L'autorité compétente communique au lanceur d'alerte le résultat final des enquêtes déclenchées par le signalement, dans le respect des dispositions nationales qui leur sont applicables.

Toute autorité qui a reçu un signalement mais qui n'est pas compétente pour traiter la violation signalée transmet le signalement, dans un délai raisonnable et de manière sécurisée, au coordinateur fédéral, qui le transmet à son tour à l'autorité compétente, et informe le lanceur d'alerte, sans délai, de cette transmission.

Si l'autorité ayant reçu le signalement sait que d'autres autorités sont également compétentes, le signalement est transmis, dans un délai raisonnable et de manière sécurisée, au coordinateur fédéral, qui le transmet aux autorités compétentes et qui en assure la coordination.

Les canaux de signalement externe doivent toujours répondre aux exigences d'indépendance et d'autonomie. Cela signifie qu'ils doivent répondre à chacun des critères suivants :

1. ils sont conçus, établis et gérés de manière à garantir l'exhaustivité, l'intégrité et la confidentialité des informations et à empêcher l'accès à ces informations aux membres du personnel de l'autorité

compétente non autorisés ;

2. ils permettent le stockage durable d'informations afin de permettre que des enquêtes complémentaires soient menées.

Les autorités compétentes sont tenues par la loi de divulguer publiquement, dans une page distincte, aisément identifiable et accessible de leur site web, tous les informations nécessaire, telles que :

- 1° les conditions pour bénéficier d'une protection ;
- 2° les coordonnées nécessaires des canaux de signalement externe, en particulier les adresses électroniques et postales, et les numéros de téléphone de ces canaux, en indiquant si les conversations téléphoniques sont enregistrées ou non ;
- 3° les procédures applicables au signalement de Violations ;
- 4° les règles de confidentialité et de respect de la vie privée ;
- 5° la nature du suivi à assurer en ce qui concerne les signalements ;
- 6° les recours et les procédures relatives à la protection contre les représailles et la possibilité pour les personnes qui envisagent d'effectuer un signalement de recevoir des conseils confidentiels ;
- 7° une déclaration expliquant clairement les conditions dans lesquelles la responsabilité des personnes qui effectuent un signalement auprès de l'autorité compétente ne serait pas engagée du fait d'une violation de la confidentialité ; et
- 8° les coordonnées du coordinateur fédéral et de l'Institut fédéral pour la protection et la promotion des droits humains.

4.3. Divulgence publique

Outre la possibilité d'effectuer un signalement par le biais des canaux de signalement interne ou externe, toute personne peut opter pour une divulgation publique des informations relatives à une violation.

Un lanceur d'alerte qui fait une divulgation publique entre en ligne de compte pour la protection visée ci-après en vertu de la présente politique si :

1. le collaborateur a d'abord effectué un signalement interne et externe, ou a effectué directement un signalement externe, mais aucune mesure appropriée n'a été prise en réponse au signalement dans les délais spécifiés ;
ou
2. le collaborateur a des motifs raisonnables de croire que :
 - a. la violation peut représenter un danger imminent ou manifeste pour l'intérêt public ; ou
 - b. en cas de signalement externe, il existe un risque de représailles ou il y a peu de chances qu'il soit véritablement remédié à la violation, en raison des circonstances particulières de l'affaire, comme lorsque des preuves peuvent être dissimulées ou détruites ou lorsqu'une autorité peut être en collusion avec l'auteur de la violation ou impliquée dans la violation.

5. Mesures de protection

Conditions de protection

Un Lanceur d'alerte bénéficie de la protection pour autant qu'il/elle :

- ait eu un motif raisonnable de croire que les informations signalées concernant la violation étaient véridiques au moment du signalement et que ces informations entraient dans le champ d'application de la présente Politique ; et
- ait effectué un signalement interne ou externe ou ait fait une divulgation publique, conformément à la présente Politique relative aux lanceurs d'alerte.

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.

Les facilitateurs et les tiers en lien avec les lanceurs d'alerte bénéficient également des mesures de protection énoncées ci-dessous s'ils avaient des motifs raisonnables de croire que le lanceur d'alerte tombait dans le champ d'application de la présente politique.

Mesures de protection contre les représailles

Si le lanceur d'alerte, le facilitateur ou un tiers en lien avec le lanceur d'alerte remplit les conditions précitées, il bénéficie d'une protection contre toute forme de représailles, en ce compris les menaces de représailles et tentatives de représailles. On entend par représailles les mesures suivantes :

1. suspension, mise à pied, licenciement ou mesures équivalentes ;
2. rétrogradation ou refus de promotion ;
3. transfert de fonctions, changement de lieu de travail, réduction de salaire, modification des horaires de travail ;
4. suspension de la formation ;
5. évaluation de performance ou attestation de travail négative ;
6. mesure disciplinaire imposée ou administrée, réprimande ou autre sanction, y compris une sanction financière ;
7. coercition, intimidation, harcèlement ou ostracisme ;
8. discrimination, traitement désavantageux ou injuste ;
9. non-conversion d'un contrat de travail temporaire en un contrat permanent, lorsque le travailleur pouvait légitimement espérer se voir offrir un emploi permanent ;
10. non-renouvellement ou résiliation anticipée d'un contrat de travail temporaire ;
11. 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 ;
12. 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 ;
13. résiliation anticipée ou annulation d'un contrat relatif à la fourniture de biens ou la prestation de services ;
14. annulation d'une licence ou d'un permis ;
15. orientation vers un traitement psychiatrique ou médical.

Aucune action civile, pénale ou disciplinaire ne peut être engagée à l'encontre des personnes qui signalent des informations sur des Violations ou font une divulgation publique conformément à la présente politique, ni aucune sanction professionnelle infligée, en raison de ce signalement ou de cette divulgation publique.

Les lanceurs d'alerte n'encourent aucune responsabilité en ce qui concerne l'obtention des informations qui sont signalées ou divulguées publiquement, ou l'accès à ces informations, à condition que cette obtention ou cet accès ne constitue pas une infraction pénale autonome.

Toute personne protégée qui s'estime victime ou menacée de représailles peut adresser une plainte motivée au coordinateur fédéral, qui engage une procédure extrajudiciaire de protection conformément aux articles 26 et suivants de 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.

Sans préjudice de tout autre recours administratif ou extrajudiciaire, toute personne protégée a le droit de former un recours en cas de représailles auprès du tribunal du travail conformément à l'article 578 du Code judiciaire.

Mesures de soutien

Chaque personne protégée a accès à des mesures de soutien et notamment aux mesures suivantes :

1. des informations et des conseils complets et indépendants, qui sont facilement accessibles et gratuits, sur les procédures et les recours disponibles en vue d'une protection contre les représailles, ainsi que sur les droits de la personne concernée, y compris ses droits au niveau de la protection des données à caractère personnel ; le lanceur d'alerte doit également être informé qu'il peut bénéficier des mesures de protection prévues par la présente loi ; des conseils techniques à l'égard de toute autorité qui est concernée par la protection du lanceur d'alerte ;
2. une assistance juridique dans le cadre des procédures pénales et civiles transfrontières conformément à la directive (UE) 2016/1919 du Parlement européen et du Conseil du 26 octobre 2016 concernant l'aide juridictionnelle pour les suspects et les personnes poursuivies dans le cadre des procédures pénales et pour les personnes dont la remise est demandée dans le cadre des procédures relatives au mandat d'arrêt européen et à la directive 2008/52/CE du Parlement européen et du Conseil du 21 mai 2008 sur certains aspects de la médiation en matière civile et commerciale et une assistance juridique 15/24 dans le cadre d'autres procédures ainsi que des conseils juridiques ou toute autre assistance juridique, conformément aux dispositions relatives à l'aide juridique de deuxième ligne et à l'assistance judiciaire ;
3. des mesures de soutien, y compris un soutien technique, psychologique, médiatique et social, pour les lanceurs d'alerte visés à l'article 6 ;
4. une assistance financière aux lanceurs d'alerte dans le cadre des procédures judiciaires.

Toute Personne Protégée peut également toujours s'adresser à l'Institut fédéral pour la protection et la promotion des droits humains pour obtenir un soutien juridique, psychologique, social, IT et de communication. L'Institut fédéral est également le point d'information central sur la protection des lanceurs d'alerte.

Coordonnées de contact :

Institut fédéral pour la protection et la promotion des droits humains, Rue de Louvain 48, 1000 Bruxelles,
adresse e-mail : info@firm-ifdh.be, voir pour plus d'informations : <https://institutfederaldroitshumains.be/fr>.

6. Sanctions en cas d'infraction à la Politique relative aux lanceurs d'alerte

Tout travailleur qui enfreint les règles de la présente Politique relative aux lanceurs d'alerte peut se voir infliger l'une des sanctions prévues par le règlement de travail. Le travailleur qui a sciemment effectué un signalement

manifestement infondé, utilisant ainsi abusivement la procédure de signalement de la présente Politique relative aux lanceurs d’alerte, peut également être sanctionné par l’une des sanctions prévues par le règlement de travail.

Les personnes associées à C.R.G. qui n’ont pas le statut de travailleurs de l’entreprise et qui ont enfreint les règles énoncées dans la présente Politique relative aux lanceurs d’alerte peuvent être sanctionnées par C.R.G. par une sanction disciplinaire.

Les lanceurs d’alerte peuvent être punis conformément aux articles 443 à 450 du Code pénal lorsqu’il est établi qu’ils ont sciemment signalé ou divulgué publiquement de fausses informations. Les personnes victimes de dommages résultant de ces signalements ou divulgations publiques ont droit à des mesures d’indemnisation conformément à la responsabilité contractuelle ou extracontractuelle.

Version : 8/09/2023