

**Directives concernant la préparation d’une politique de signalement et exemple de politique de signalement**

***Dernière mise à jour [2023]***

Une entreprise est tenue de conserver une documentation écrite sur la mise en place d’un dispositif de signalement et des procédures y afférentes. Ainsi, l’entreprise doit, au minimum, élaborer une politique de signalement et une procédure écrite pour le traitement des signalements.

À la page 4, nous présentons un exemple de politique de signalement qui peut être mis en œuvre après quelques adaptations. Si vous souhaitez élaborer votre propre politique en matière de signalement, les éléments suivants doivent ou devraient être pris en compte au minimum :

**1. Description initiale du système, y compris sa finalité et son contexte**

Une section d’introduction peut présenter une description générale de la finalité et du contexte de l’instauration du système.

En outre, un cadre initial peut être donné à la manière dont l’entreprise traite les affaires des employés, en précisant que le dispositif de signalement doit fonctionner comme un complément aux communications directes et quotidiennes sur le lieu de travail concernant les manquements et les questions insatisfaisantes.

**2. Qui peut effectuer un signalement ?**

Le système sera normalement destiné à être utilisé par les employés, les partenaires et les employés des partenaires pour signaler, en toute bonne foi, des préoccupations et des soupçons fondés concernant l’entreprise, ses employés et ses partenaires. Les partenaires associés à l’entreprise peuvent, par exemple, être des clients, des fournisseurs ou des consultants externes.

Il peut également être envisagé de permettre au système d’inclure les signalements d’anciens employés, de la direction actuelle et précédente, et d’autres personnes extérieures.

**3. Que peut-on déclarer dans le cadre de ce système ?**

La politique doit déterminer quelles affaires peuvent être signalées par le biais du système, y compris ce qui peut et ne peut pas être signalé.

La directive couvre le signalement d’infractions à un certain nombre de règles juridiques de l’UE. Plusieurs pays ont indiqué qu’ils étendront également le dispositif pour couvrir, par exemple, les infractions pénales, notamment la violation de la confidentialité, les malversations, le vol, la fraude, l’escroquerie, le détournement de fonds et la corruption, le harcèlement sexuel et d’autres formes graves de harcèlement au travail. La législation n’est pas encore en place dans certains pays. Nous mettrons régulièrement à jour le guide au fur et à mesure que chaque pays adoptera la législation.

En outre, l’inclusion d’autres comportements indésirables dans l’option de signalement peut être envisagée, en fonction de la situation de l’entreprise.

À cet égard, on peut envisager de préparer une liste positive et une liste négative d’affaires qui entrent et n’entrent pas, respectivement, dans le champ d’application du système.

La question de savoir qui peut faire l’objet d’un signalement peut également être envisagée. Cela s’applique généralement aux employés de l’entreprise, y compris la direction, les administrateurs, les membres du conseil d’administration, les comptables, les avocats, les clients, les consultants, les fournisseurs, etc. et d’autres tiers liés à l’entreprise.

**4. Comment organiser le système ?**

Il convient d’examiner comment le système doit être organisé au sein de l’entreprise. L’organisation détaillée dépend naturellement, entre autres, de la localisation, de la structure, de la taille, de la nature et du secteur d’activité de l’entreprise.

À cet égard, il convient de se demander qui est responsable de la réception des signalements. Il peut souvent y avoir un risque de conflits d’intérêts ; c’est pourquoi il sera approprié pour une entreprise de confier les signalements à une fonction externe indépendante qui possède l’expertise et les compétences nécessaires pour traiter tous les types de signalements.

Il conviendra généralement de mettre en place une équipe ou une fonction spécifique dans l’entreprise, à un niveau approprié ou avec les qualifications nécessaires, qui pourra travailler avec un expert externe pour traiter les différents types de signalements reçus.

Un manuel devrait être préparé pour traiter les différents types de signalement de manière optimale en fonction de l’auteur du signalement, de ce qui est signalé et de qui fait l’objet du signalement.

**5. Comment faire des signalements via le système d’alerte ?**

Dans une politique de signalement, il convient de décrire précisément, à l’intention des lanceurs d’alerte potentiels, la manière dont un signalement peut être effectué par l’intermédiaire du dispositif de signalement, en indiquant, par exemple, qui fournit la solution informatique, comment elle fonctionne, quelles langues sont disponibles, si le signalement doit être effectué de manière anonyme ou nominative, et d’autres questions pratiques.

Il convient également de décrire la manière dont les pièces justificatives peuvent être soumises et comment se déroule la communication avec un éventuel lanceur d’alerte.

**6. Que faut-il appliquer en matière de confidentialité et d’anonymat ?**

Une politique de signalement devrait décrire ce qui s’applique au sein du dispositif de signalement en matière de confidentialité et d’anonymat.  La loi prévoit une option spéciale permettant de traiter les données à caractère personnel lorsque cela est nécessaire pour traiter les signalements dans le cadre du système. Cela devrait être décrit dans une politique de signalement.

Les entreprises peuvent traiter des données non sensibles conformément au RGPD, des données personnelles sensibles et des données relatives à des infractions pénales lorsque cela est nécessaire pour traiter les signalements reçus dans le cadre du dispositif de signalement.

Une politique de signalement doit également indiquer que les autres règles et principes du RGPD – qui doivent toujours être respectés – doivent également être observés dans une situation de signalement. Il en va de même pour les procédures à suivre lors d’éventuelles enquêtes consécutives aux signalements. Toutefois, il sera possible de divulguer les informations dans certaines conditions, notamment lorsque cela est nécessaire pour prévenir des violations de la loi et autres actes répréhensibles.

La politique peut aussi indiquer que la loi protège les lanceurs d’alerte contre les représailles, par exemple, lorsque la personne en question signale des faits dont elle a eu connaissance en rapport avec des affaires relatives à son travail et à l’entreprise.

La loi prévoit qu’aucune mesure de représailles ne peut être prise à l’encontre des lanceurs d’alerte, qu’il s’agisse de licenciement, de mutation, de réduction de salaire, de harcèlement, etc.

Les lanceurs d’alerte qui ont fait l’objet de représailles pour avoir dénoncé des faits ont droit à une indemnisation spéciale.

Il convient également d’indiquer dans une politique comment, et selon quelles procédures, la conservation et la suppression des données à caractère personnel sont effectuées, ainsi que le responsable du traitement des données en relation avec le dispositif de signalement.

**7. Quelles sont les procédures à suivre lorsqu’un lanceur d’alerte signale quelque chose ?**

Une politique doit inclure une description des procédures applicables lorsqu’un lanceur d’alerte signale quelque chose. Cela comprend les éléments suivants :

* comment la solution technique fonctionne du point de vue d’un lanceur d’alerte,
* les délais pour accuser réception d’un signalement,
* les délais de réception du retour d’information,
* des conseils à l’intention des lanceurs d’alerte potentiels sur la possibilité de faire un signalement via des dispositifs externes.

Un manuel détaillé doit être préparé à usage interne de l’entreprise sur le type de traitement appliqués aux différents signalements dans le cadre de la collaboration entre la direction de l’entreprise, les employés concernés de l’entreprise et les experts externes.

**8. Quels sont les droits des personnes faisant l’objet d’un signalement ?**

Une politique doit normalement décrire les droits des personnes ayant fait l’objet d'un signalement, et doit comporter une description plus détaillée de la manière dont ces employés doivent être traités.

Les personnes auxquelles les informations se rapportent seront normalement notifiées si des informations sont fournies à leur sujet. La personne recevra ainsi une notification lorsque l’affaire est abandonnée si elle est manifestement infondée, et elle sera impliquée dans le processus si l’affaire se poursuit effectivement. À cet égard, la personne a le droit de demander la correction, la suppression ou la limitation des informations.

**9. Quels sont les droits des employés qui mènent ou contribuent à des enquêtes ?**

La politique doit également énoncer les droits des employés qui contribuent au dispositif de signalement dans le cadre des enquêtes menées ou des informations fournies, y compris le fait qu’ils sont protégés contre les conséquences négatives sur leur emploi résultant de leur contribution.

**10. Qui peut-on contacter en cas de doute sur le dispositif de signalement ?**

Une politique doit enfin déterminer qui peut être contacté en cas de doute sur des questions concernant le dispositif de signalement.

**Politique de signalement pour les employés [à adapter]**

***Dernière mise à jour [2023]***

**Contexte et finalité**

[NOM DE L'ORGANISATION] (ci-après « l’organisation ») met à la disposition de ses employés un dispositif de signalement.

Un dispositif de signalement est un canal indépendant par lequel les employés peuvent signaler des soupçons ou rapporter des informations spécifiques concernant des violations graves ou d’autres affaires sérieuses au sein de l’organisation.

Le dispositif de signalement doit être considéré comme un complément à la possibilité que vous avez, en tant qu’employé, de vous adresser à un membre de la direction si vous constatez des fautes ou des points d’insatisfaction sur lesquels vous souhaitez attirer l’attention.

Cette politique de signalement décrit plus en détail quand vous pouvez utiliser le dispositif de signalement, ce que vous pouvez signaler, comment un signalement est traité, les droits des personnes mises en cause, etc.

**Contenu :**

1. [Qui peut faire un signalement via le dispositif de signalement ?](bookmark://_Hvem_kan_indberette)
2. [Qui peut faire l’objet d’un signalement ?](bookmark://_Hvem_kan_der)
3. [Quelles sont les affaires pouvant faire l’objet d’un signalement ?](bookmark://_Hvilke_forhold_kan)
4. [Comment faire un signalement ?](bookmark://_Hvordan_foretages_indberetning?)
5. [Qui reçoit les signalements ?](bookmark://_Hvem_modtager_indberetninger?)
6. [Procédure de réception d’un signalement](bookmark://_Procedure_ved_modtagelse)
7. Enquête sur un signalement
8. [Devoir de confidentialité et divulgation d’informations](bookmark://_Tavshedspligt_og_videregivelse)
9. Anonymat, protection contre les représailles et autres droits pour un lanceur d’alerte
10. Délais et communication continue
11. [Confidentialité](bookmark://_Fortrolighed)
12. [Enregistrement des signalements](bookmark://_Registrering_af_indberetninger)
13. Droits des personnes mises en cause
14. [Dispositif de signalement externe à l’Agence danoise de protection des données](bookmark://_Ekstern_whistleblowerordning_hos)
15. [Le droit de publication du lanceur d’alerte](bookmark://_Whistleblowerens_ret_til)
16. Système de

Outre ces informations, l’organisation a élaboré une politique de confidentialité qui concerne spécifiquement le traitement des données à caractère personnel dans le cadre du dispositif de signalement. Elle peut être consultée ici : [insérer le lien].

**1. Qui peut faire un signalement via le dispositif de signalement ?**

Le dispositif de signalement s’applique à tous les employés de l’organisation. Il s’applique également aux personnes ayant un emploi à durée déterminée ou au personnel temporaire.

*Exemples d'autres groupes cibles auxquels vous pourriez choisir d’étendre le dispositif : [*membres du conseil d’administration, actionnaires, membres du conseil de surveillance, consultants, fournisseurs, entrepreneurs, commissaires aux comptes, etc.].

**2. Qui peut faire l’objet d’un signalement ?**

Le dispositif de signalement doit être utilisé pour rapporter des informations et signaler des affaires relatives à des violations et des manquements graves par des employés ou d’autres personnes associées à l’organisation. Ces autres personnes peuvent être, par exemple, des membres du conseil d’administration, des actionnaires, des membres du conseil de surveillance, des consultants, des fournisseurs, des donneurs d’ordre, des commissaires aux comptes, etc.

**3. Quelles sont les affaires pouvant faire l’objet d’un signalement ?**

Les violations du droit communautaire, les violations graves du droit national et d’autres faits graves peuvent être signalés, pour autant qu’ils concernent des personnes liées à l’organisation (voir plus haut).

Un signalement peut porter sur une suspicion ou une connaissance réelle de violations dans les domaines suivants, par exemple :

* Marchés publics/appels d’offres
* Blanchiment de capitaux et financement du terrorisme
* Protection de la vie privée et sécurité des réseaux et des systèmes d’information
* Protection des consommateurs
* Criminalité économique, telle que détournement de fonds, vol, corruption, fraude et falsification
* Piratage, écoutes, enregistrement de conversations entre tiers, etc.
* Violations de la législation en matière de comptabilité, de fiscalité, etc.
* Violation de la confidentialité
* Négligence de l’obligation légale d’agir
* Violation des règles relatives à l’usage de la force
* Violations graves et répétées des principes juridiques
* Tromperie délibérée des citoyens et des partenaires
* Violence physique et psychologique et abus sexuel ou harcèlement grave fondé, par exemple, sur la race, le sexe, la langue, la fortune, l’origine nationale ou sociale, l’affiliation politique ou religieuse
* Négligence des normes professionnelles susceptible de constituer un risque pour la sécurité et la santé des personnes, par exemple
* Défaut de soins
* Violations graves ou répétées des directives internes du lieu de travail concernant, par exemple, les voyages d’affaires, les cadeaux et les rapports financiers
* Défauts graves et irrégularités graves liés à l’exploitation informatique ou à la gestion du système informatique.

Ce qui précède est une liste non exhaustive d’exemples.

Le dispositif de signalement ne s’applique pas aux informations de nature triviale ou aux informations concernant, par exemple, la violation des directives internes relatives aux congés de maladie, au tabagisme, à l’alcool, à l’habillement, à l’utilisation privée des fournitures de bureau, ou la violation de règles accessoires, telles que le non-respect des exigences en matière de documentation.

Toutefois, dans le cas de violations systématiques, il se pourrait bien que ces questions, par ailleurs moins graves, soient couvertes par le dispositif de signalement. Ce dernier ne peut pas être utilisé pour signaler votre propre relation de travail, notamment les conflits entre employés, les problèmes de coopération ou les questions qui relèvent du droit syndical (le harcèlement aggravé et le harcèlement sexuel sont toutefois couverts, voir ci-dessus, et les problèmes de coopération sont couverts s’ils sont jugés suffisamment graves pour présenter un risque réel pour la vie et la santé humaines).

Les informations sur des violations ou des affaires qui ont eu lieu avant la mise en place par l’organisation d’un dispositif de signalement peuvent être signalées.

**4. Comment faire un signalement ?**

Les employés de l'organisation peuvent effectuer des signalements anonymes par écrit via une solution numérique, qui est gérée par un fournisseur externe.

Vous trouverez un lien vers le dispositif de signalement ici : <https://nordicwhistle.whistleportal.eu/>.

Pour en savoir plus sur la procédure de signalement, cliquez ici :[insérer un lien vers le Guide d’utilisation du système d’alerte – Whistleblower].

**5. Qui reçoit les signalements ?**

Les informations contenues dans un signalement sont reçues par Whistleblower Partners Response Team qui traite les signalements reçus via le dispositif de signalement de l’organisation. Whistleblower Partners Response Team (ci-après le « référent ») est un conseiller externe et indépendant. Lorsque le référent a reçu un signalement :

* il examine le signalement, et détermine aussi quel niveau de l’entreprise est concerné,
* il accuse réception du signalement au lanceur d’alerte,

*À adapter en fonction de l’organisation choisie pour le dispositif de signalement – supprimer la totalité de la section a ou b, selon ce qui n’est pas pertinent.*

*(couvert par la convention d’examen de Whistleblower Partners Response Team) :*

* a. [le référent transmet le dossier à la personne de contact pertinente au sein de l’organisation, en fonction de l’individu faisant l’objet du signalement.

Avant de communiquer le signalement à la personne de contact pertinente au sein de l’organisation, le référent s’assure que le signalement ne concerne pas la personne de contact et que celle-ci n’a pas de conflit d’intérêts en rapport avec le traitement du signalement.

Si tel est le cas, le signalement sera partagé avec une autre personne de l’organisation que le référent juge compétente pour traiter le signalement en question.]

*(non couvert par la convention d’examen de Whistleblower Partners* *Response Team – nécessite un accord séparé avec Whistleblower Partners. Contactez-nous si vous le souhaitez :*

* *b.*[le référent traite la question.]]

Nous avons choisi cette solution particulière parce que nous voulons créer le plus grand sentiment de sécurité possible pour les employés de l’organisation dans le cadre d’un signalement.

**6. Procédure de réception d’un signalement**

À la réception d’un signalement, une évaluation est effectuée pour savoir s’il entre dans le champ d’application du dispositif de signalement (cf. section 3).

Si le rapport ne relève pas du champ d'application du dispositif de signalement, il sera rejeté et ne pourra donc pas être traité dans ce cadre-là.

Si un rapport ne relève pas du champ d’application du dispositif de signalement, le lanceur d’alerte recevra des conseils sur la manière dont il peut aborder la question au sein de l’organisation.

**7. Enquête sur un signalement**

*Si la solution a. est retenue à la section 5, insérer « la personne de contact pertinente au sein de l’organisation ». Si la solution b. est choisie à la section 5, insérer « Référent » :*

Une fois que[insérer] a reçu le signalement,[insérer] doit effectuer un suivi approfondi qui, selon les circonstances entourant le signalement, peut inclure :

* Le lancement d’une enquête interne pour confirmer ou infirmer l’exactitude des informations contenues dans un signalement
* Un briefing de la direction ou du conseil d’administration de l’organisation
* Un signalement à la police ou à l’autorité de surveillance compétente
* Une décision quant aux réponses à apporter, par exemple en vertu du droit du travail ou du droit des contrats
* La clôture de l’affaire

[insérer] est chargé de demander que le rapport fasse l’objet d’une enquête approfondie et de prendre les mesures nécessaires à cet égard.

Ensuite, [insérer] doit préparer une déclaration à l’intention de la direction, qui décidera alors de la réponse à apporter, qu’il s’agisse d’un signalement aux autorités ou d’autres réponses en vertu du droit du travail ou du droit des contrats.

Enfin, un retour d’information doit être donné au lanceur d’alerte dans le délai de 3 mois prévu par le dispositif de signalement (cf. section 10 ci-dessous).

**8. Devoir de confidentialité et divulgation d’informations**

Seul le référent *À garder si la solution 5.a. est sélectionnée dans la section 5 :* [et la personne de contact pertinente dans l’organisation ont] a accès aux informations contenues dans un signalement. Les rapports sont soumis à un devoir particulier de confidentialité, et leur contenu ne peut donc pas être divulgué à d’autres personnes.

L’obligation spéciale de confidentialité ne s’applique qu’aux informations contenues dans un rapport ; si d’autres informations apparaissent dans le cadre d’une enquête ultérieure, ces informations ne sont pas couvertes par l’obligation spéciale de confidentialité. Dans ce cas précis, les règles générales de divulgation et d’accès aux documents s’appliquent.

Si le lanceur d'alerte a renoncé à son anonymat, l’obligation spéciale de confidentialité ne s’applique plus aux informations incluses dans le rapport. De même, l’organisation a le droit de partager les informations issues d’un rapport, y compris l’identité du lanceur d’alerte, si elles sont connues, de la police, par exemple. Dans ce cas, le lanceur d’alerte doit en être informé.

**9. Anonymat, protection contre les représailles et autres droits du lanceur d’alerte**

En tant que lanceur d'alerte, vous avez le droit de rester anonyme tout au long de la procédure. La solution informatique choisie offre la possibilité de communiquer de manière anonyme avec le référent alerte.

Toutefois, un rapport peut être d’une nature telle qu’il peut être difficile d’enquêter de manière approfondie sur une affaire sans que le lanceur d’alerte choisisse de se manifester et renonce ainsi à son droit à l’anonymat. C’est au lanceur d’alerte lui-même de décider si cela doit se produire. Si l’anonymat est levé, l’intention de la directive sur les lanceurs d’alerte est de protéger le lanceur d’alerte contre, entre autres, toute forme de représailles ou de menaces, ou de tentatives de représailles, qui se produisent à la suite d’un signalement effectué par le lanceur d’alerte. Les représailles doivent être comprises comme tout type de traitement défavorable ou de conséquence négative qui se produit en réaction à un signalement. Cela peut prendre la forme, par exemple, de : suspension, licenciement, rétrogradation ou absence de promotion, transfert de fonctions, mutation, réduction de salaire, mesure disciplinaire, contrainte, intimidation, harcèlement, discrimination, etc.

Le fait d’être mentionné dans un signalement peut avoir des conséquences importantes : le lanceur d’alerte est donc tenu d’agir de bonne foi quant au contenu du rapport. Un signalement délibérément faux de la part d’un lanceur d’alerte, par exemple en matière de harcèlement, peut entraîner des conséquences pénales à son encontre.

En revanche, un lanceur d’alerte ne peut être tenu responsable de la divulgation d’informations confidentielles s’il avait des motifs *raisonnables* de croire que les informations divulguées sous la forme d’un signalement étaient correctes au moment du signalement, et que les informations concernaient des violations graves ou d’autres sujets sérieux couverts par le dispositif.

Sur cette base, le lanceur d’alerte ne sera pas non plus tenu responsable d’avoir eu accès aux informations ayant fait l’objet du signalement. Cela présuppose toutefois que l’acte par lequel cet accès a été obtenu ne constitue pas en soi un acte délictueux, par exemple un cambriolage.

**10. Délais et communication continue**

Le référent gère la communication avec le lanceur d’alerte via le système d’alerte.

Le lanceur d’alerte doit recevoir une confirmation de la réception de son signalement au plus tard 7 jours après l’avoir effectué.

En outre, le lanceur d’alerte doit recevoir un retour d’information dès que possible, et au plus tard dans les trois mois suivant l’accusé de réception ; cela signifie que – dans la mesure du possible – le lanceur d’alerte doit être informé des mesures qui ont été prises, ou qu’il est prévu de prendre, et de la raison pour laquelle ce type de suivi spécifique a été choisi. En ce qui concerne le retour d’information, certaines informations ne peuvent être partagées avec le lanceur d’alerte, par exemple en raison d’une obligation légale de confidentialité, de la législation sur les données à caractère personnel, etc.

Outre les informations sur le suivi choisi, le lanceur d’alerte doit, dans la mesure du possible, être informé du déroulement de l’enquête et de son résultat, si cela est possible dans le cadre des règles applicables.

Si, en raison des circonstances de l’affaire, il n’est pas possible de donner un retour d'information définitif avant l’expiration du délai de trois mois, le lanceur d’alerte doit en être informé, ainsi que de la date à laquelle un retour d’information supplémentaire peut être attendu.

Comme cela a été mentionné, un lanceur d’alerte peut choisir de se manifester, et dans ce cas, il peut être pertinent d’organiser des réunions physiques avec le référent *À garder si la solution a. est choisie dans la section 5 :*[et la personne de contact pertinente dans l’organisation].

**11. Confidentialité**

Le dispositif de signalement est conçu et géré de manière à garantir la confidentialité de l’identité du lanceur d’alerte et de toute personne susceptible d’être mentionnée dans un rapport.

Le système informatique utilisé pour gérer le dispositif de signalement est soumis à un certain nombre d’exigences strictes en matière de sécurité qui garantissent, entre autres, l’anonymat et la confidentialité. Cela signifie que la personne qui fait un signalement via le dispositif de signalement est, et reste, anonyme si elle le souhaite. Cela signifie également que le système n’enregistre pas les adresses IP, que les métadonnées sont supprimées de tous les fichiers téléchargés et que la transmission et le stockage de toutes les données sont cryptés.

Le référent *À conserver si la solution a. est sélectionnée dans la section 5 :*[et la personne de contact pertinente dans l’organisation sont] est soumis à un devoir de confidentialité ; des restrictions d’accès ont été mises en place pour toutes les informations relatives à un signalement.

**12. Enregistrement des signalements**

Les signalements reçus, y compris les documents les accompagnant, doivent être enregistrés (stockés systématiquement) afin de garantir leur accessibilité et, le cas échéant, leur utilisation comme preuves dans tout procès ultérieur. En même temps, l’enregistrement donne également l’assurance que tous les signalements concernant la même affaire sont identifiés et peuvent conduire à une enquête plus approfondie. Cet enregistrement se fait dans le système d’alerte.

Les rapports sont conservés aussi longtemps que cela est nécessaire et proportionné. Les principes de conservation sont décrits plus en détail dans la politique de confidentialité de l’organisation concernant le dispositif de signalement.

**13. Droits des personnes concernées**

Toute personne mentionnée dans un signalement a le droit de voir son identité protégée dans le cadre du traitement de l’affaire. En outre, les personnes concernées doivent avoir accès à une défense efficace, ce qui est assuré entre autres par l’enregistrement d’un rapport et donc par la documentation des affaires mentionnées.

Les personnes concernées disposent également d’un certain nombre de droits dans le cadre du traitement de leurs données à caractère personnel. Toutefois, le devoir de confidentialité de l’organisation entraîne des restrictions quant au moment où les personnes concernées doivent être informées du traitement des informations, et quant à la possibilité d’invoquer leur droit d'accès, d’effacement, etc.

Si un signalement conduit à l’introduction d’une action en justice, la personne concernée par le signalement a le droit de bénéficier d’une procédure consultative ou d’accéder aux dossiers concernant les informations contenues dans un signalement. Toutefois, si le lanceur d’alerte est anonyme, il n’y a pas de droit d’accès à son identité.

**14. Dispositif de signalement externe**

En vertu de la directive sur les lanceurs d’alerte, il incombe à l’organisation d’informer ses employés des dispositifs de signalement externes suivants, qui peuvent être utilisés comme alternative au dispositif interne de l’organisation :

[Insérer une description des dispositifs nationaux de signalement externes mis en place dans le pays de l’organisation].

Vous trouverez plus d’informations sur la manière de faire un signalement par l’intermédiaire du dispositif de signalement chez [insérer le nom de l’organisation responsable du dispositif de signalement externe] ici : [Insérer le lien vers les informations sur la procédure de signalement au dispositif de signalement externe].

Les employés de l’organisation ont la liberté de choisir s’ils veulent signaler un problème au dispositif interne de signalement de l’organisation ou à un dispositif externe. Toutefois, l’organisation encourage ses employés à utiliser son dispositif de signalement dans les cas où l’employé estime que la violation suspectée peut être traitée efficacement en interne et qu’il n’y a pas de risque de représailles.

La possibilité d’utiliser au choix le dispositif interne ou un dispositif externe ne limite pas la liberté d’expression habituelle des employés.

**15. Le droit de publication du lanceur d’alerte**

La directive sur les lanceurs d’alerte et la protection que les règles accordent aux lanceurs d’alerte s’appliquent également à la publication par un lanceur d’alerte d’informations mentionnées dans un signalement.

Toutefois, il est indispensable que le lanceur d’alerte

* ait fait, avant la publication, un signalement à la fois au dispositif de signalement interne de l’organisation et à un dispositif de signalement externe sans qu’aucune mesure appropriée n’ait été prise, ou
* ait des motifs raisonnables de croire que la violation en question constitue un danger imminent ou évident pour l’intérêt public, ou
* ait des raisons de croire que le fait de s’adresser au dispositif de signalement externe entraînera un risque de représailles, ou que l’affaire ne sera pas traitée efficacement en raison de ses circonstances particulières.

**16. Système de divulgation *(ne conserver cette section que si l’organisation est une autorité publique)***

En tant qu’autorité publique, l’organisation doit, au moins une fois par an, publier un état des signalements reçus conformément à la directive sur les lanceurs d’alerte, comprenant :

* Le nombre de signalements et leurs thèmes généraux
* Quel pourcentage des signalements

1) a fait l’objet d’un examen actif,

2) a été rejeté ou clôturé, et

3) a donné lieu à un signalement à la police, en termes absolus.