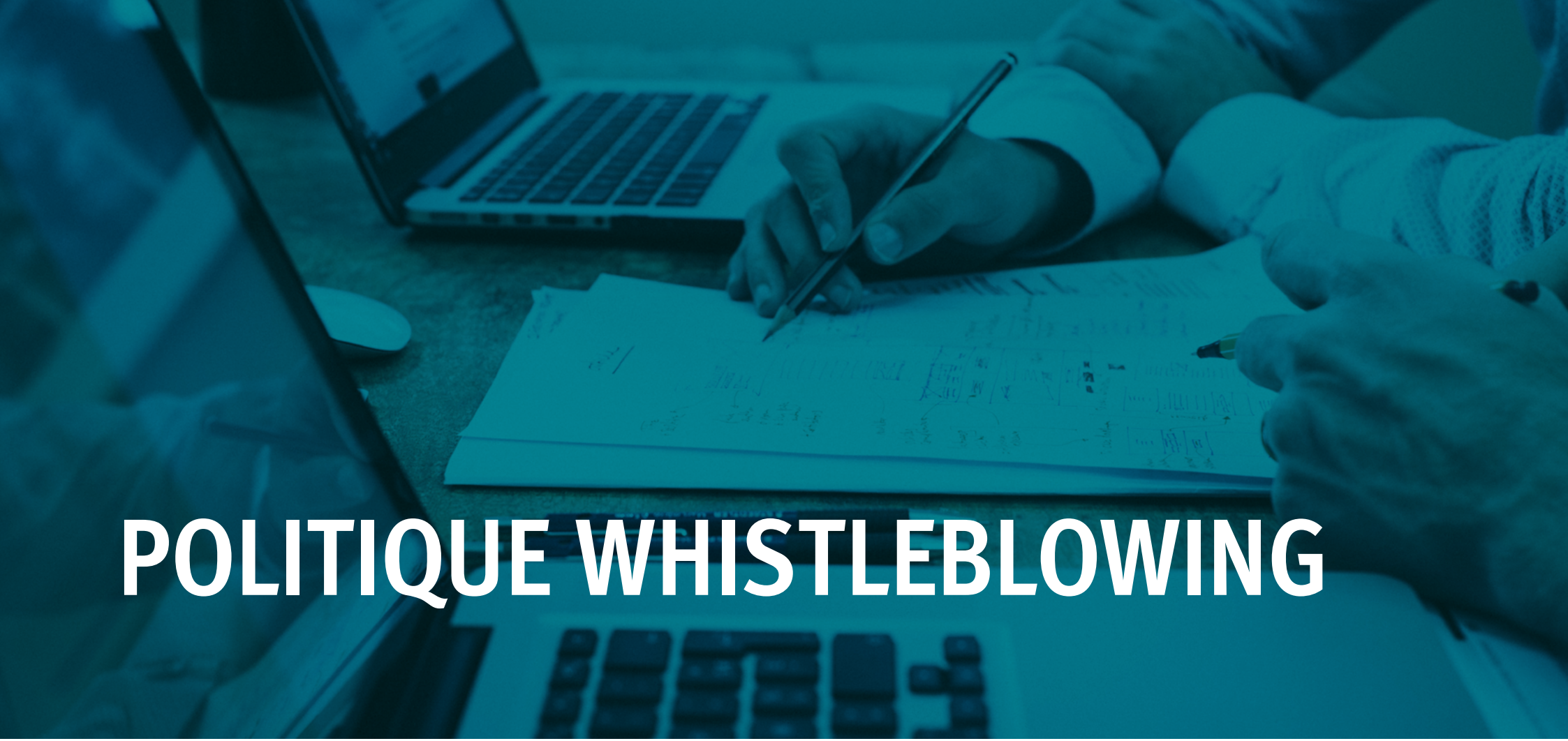

# POLITIQUE WHISTLEBLOWING

JUIN 2023

ethias

# CONTENU


1. CADRE GÉNÉRAL 3

2. CARACTÉRISTIQUES D'UN SIGNALEMENT INTERNE 4

2.1. Dans quels cas introduire un signalement ? 4

2.2. A qui s'adresser et comment introduire un signalement interne ? 4

2.3. Qui peut introduire un signalement ? 5

2.4. Le signalement peut-il être anonyme ? 5

3. GARANTIES ET EFFETS DE LA PROTECTION DU LANCEUR D'ALERTE 6

3.1. Qui bénéficie des mesures de protection ? 6

3.2. Quelles sont les mesures de protection ? 7

3.3. Mesures de soutien 8

3.4. Exonération de la responsabilité pénale 8

4. MESURES DE PROTECTION DES PERSONNES CONCERNÉES 9

4.1. Confidentialité 9

4.2. Indemnisation 9

5. SIGNALEMENT INTERNE VS SIGNALEMENT EXTERNE 10

5.1. Dispositif d'Alerte interne en pratique 10

5.2. Signalement externe : déclenché en dehors d'Ethias 13

6. TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL 14

# 1. CADRE GÉNÉRAL

Ethias s'engage à exercer ses activités avec la plus grande intégrité et attend, de chacun de ses collaborateurs, qu'il adopte un comportement professionnel irréprochable, dans le respect des lois mais également des valeurs de l'entreprise et des règles de conduite qu'elle s'est assignée.

Dans ce contexte, une personne qui constate ou soupçonne qu'un membre du personnel d'Ethias a un comportement inapproprié, contraire à l'éthique (qui contreviendrait à l'une des règles de conduite décrites dans la Politique d'Intégrité ou le Code de déontologie d'Ethias) ou illégal – doit avoir la possibilité, dans un climat de confiance, de signaler ces pratiques, fautes, dysfonctionnements ou actes qu'il estime inappropriés, contraires à l'éthiques ou illégaux via une procédure interne ou externe dont l'exécution est strictement encadrée.

La mise en place d'un tel dispositif de signalement[1] requiert de trouver des équilibres délicats pour rencontrer des finalités plurielles. Il s'agit, en effet, tout à la fois d'assurer le respect de la réglementation et des règles internes par un contrôle interne solide, de protéger l'image d'Ethias (en évitant un signalement externe ou public) et de préserver un climat serein au sein de l'entreprise.

L'objectif de la présente politique est de déterminer la procédure à suivre lorsqu'on souhaite bénéficier de la protection due aux lanceurs d'alerte lors du signalement d'un comportement inadéquat dans le chef d'un collaborateur d'Ethias et d'établir un cadre contraignant à respecter et des garanties, notamment de confidentialité.

Un tel système complète, sans s'y substituer, les canaux existants de signalement de fautes ou dysfonctionnements via, notamment, la hiérarchie ou l'audit interne.

Ce dispositif doit s'attacher à la protection tant de la personne qui recourt à la procédure de dénonciation que de la personne mise en cause, notamment en ce qui concerne la présomption d'innocence et le traitement de ses données personnelles.

La politique de Whistleblowing est soumise à la validation du comité de direction et à l'approbation du conseil d'administration. Elle fait l'objet d'une mise à jour trisannuelle (sauf changement majeur à y intégrer), avec une revue annuelle par la compliance (avec info au CD/CA le cas échéant).

1 Cadre juridique principal :
Loi belge du 28 novembre 2022 qui transpose la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union ou au droit national constatées au sein d'une entité juridique du secteur privé.

# 2. CARACTÉRISTIQUES D'UN SIGNALEMENT INTERNE

## 2.1. DANS QUELS CAS INTRODUIRE UN SIGNALEMENT ?

Cette procédure concerne, dans un contexte professionnel les signalements portant sur des faits ou des menaces passés, actuels ou à venir, **toute forme de non-respect, d'irrégularité ou d'inconduite réelle ou présumée au sein d'Ethias qui conduit ou pourrait conduire, de manière non limitative, à une violation de dispositions légales, réglementaires ou prudentielles et de nos valeurs et règles de conduite sur le plan de l'intégrité des activités d'Ethias**.

Le mécanisme de signalement doit toutefois être limité aux « faits ou situations suffisamment graves qui doivent être signalés dans l'intérêt public ou dans l'intérêt de la bonne gouvernance de l'entreprise ».

Un signalement peut notamment concerner une violation des règles applicables en matière de : marchés publics ; services, produits et marché financiers (lois et règlements surveillés par la BNB ou la FSMA, telle que l'information correcte des clients, les conflits d'intérêts, la bonne gouvernance, le fit & proper etc.); protection des consommateurs ; lutte contre la fraude fiscale ou sociale ; prévention du blanchiment de capitaux et du financement du terrorisme ;...

Chaque déclaration intervient sur une base volontaire. La procédure de signalement est facultative.

Par ailleurs, ce dispositif ne se substitue pas aux autres possibilités qui existent déjà dans l'entreprise. Il s'agit, en effet, d'un dispositif complémentaire qui, sans s'y substituer, complète les autres canaux existants (qui ne sont, quant à eux, pas considérés comme des signalements internes rentrant dans le champ d'application de la présente procédure et des protections corrélatives).

## 2.2. A QUI S'ADRESSER ET COMMENT INTRODUIRE UN SIGNALEMENT INTERNE ?

Le **Head of Compliance** a été désigné par Ethias en tant que « Gestionnaire des signalements ». Il s'agit d'une personne indépendante, impartiale, compétente pour recevoir les signalements en toute discrétion, centraliser les informations et pour en assurer le suivi.

Le lanceur d'alerte peut introduire son signalement interne en utilisant le bouton d'alerte « Whistleblower» disponible tant sur l'Intranet que sur le site Web Corporate d'Ethias. Par ailleurs, il peut introduire son signalement par écrit, en utilisant soit l'e-mail à l'adresse whistleblowing@ethias.be soit un courrier papier adressé directement au Head of Compliance, rue des Croisiers, 24 à 4000 Liège, avec la mention « confidentiel ».

Dans le cas où la préoccupation concerne le Head of Compliance, le lanceur d'alerte doit alors rapporter le signalement au **Chief Executive Officer** de l'entreprise (son adresse e-mail étant potentiellement consultée par son secrétariat, il convient de privilégier un contact direct pour assurer la confidentialité).

## 2.3. QUI PEUT INTRODUIRE UN SIGNALEMENT ?

**Dans un contexte professionnel**, le dispositif de signalement interne d'Ethias s'adresse et peut être utilisé par :

- tous les collaborateurs Ethias, à tout niveau hiérarchique, qu'ils soient travailleurs salariés, indépendants, consultants, actionnaires, membres de l'organe d'administration, de direction ou de surveillance y compris les membres non exécutifs, ainsi que les bénévoles et stagiaires rémunérés ou non rémunérés et ce, même si la relation de travail a pris fin au moment de la divulgation ;
- les personnes en cours de recrutement, dont la relation de travail n'a pas encore commencé dans les cas où des informations sur des violations ont été obtenues lors du processus de recrutement ou d'autres négociations précontractuelles ;
- toute personne travaillant sous la supervision et la direction de contractants, de sous-traitants et de fournisseurs.

**En dehors d'un contexte professionnel**, la procédure est également applicable aux lanceurs d'alerte lorsqu'ils signalent une infraction aux dispositions prévues dans les domaines des services financiers et d'Anti-Money Laundering.

## 2.4. LE SIGNALEMENT PEUT-IL ÊTRE ANONYME ?

Oui, le signalement anonyme est autorisé de sorte que le lanceur d'alerte peut choisir de dévoiler son identité ou de rester anonyme, y compris à l'égard du Head of Compliance.

Ethias a implémenté, sur son Intranet et sur son site Internet, une solution de bouton d'alerte « whistleblower » qui garantit l'anonymat du lanceur d'alerte, ainsi que la confidentialité et la sécurité des échanges. Cette solution permet également de contacter le lanceur d'alerte en cas de question complémentaire ou afin de l'informer quant au suivi diligent du dossier.

Pour ceux qui ne désirent pas utiliser ce bouton d'alerte, il leur est possible d'introduire un signalement anonyme par courrier. Cependant, d'un point de vue pratique, ce signalement anonyme est vivement déconseillé : en effet, cet anonymat risque de rendre impossible tout échange entre le lanceur d'alerte et le Gestionnaire du signalement, notamment quand Ethias doit informer le lanceur du suivi du dossier.

# 3. GARANTIES ET EFFETS DE LA PROTECTION DU LANCEUR D'ALERTE

## 3.1. QUI BÉNÉFICIE DES MESURES DE PROTECTION ?

### LES LANCEURS D'ALERTE

Les premiers concernés sont les lanceurs d'alerte, qui bénéficient de la protection prévue par la loi et par la présente procédure s'ils sont de BONNE FOI.

Pour être de bonne foi : il faut et il suffit que le lanceur d'alerte ait eu des **motifs raisonnables** de croire, à la lumière des circonstances et des informations dont il dispose au moment du signalement, à la véracité des informations signalées, en vue de protéger ce qu'il estime être le bien commun, l'intérêt général (Critère de la croyance raisonnable). Des rumeurs ou des ragots ne sont pas suffisants.

Il importe d'apprécier ce critère au regard d'une personne placée dans une situation similaire et disposant de connaissances comparables. Ce faisant, le lanceur d'alerte ne devrait pas perdre le bénéfice de la protection au seul motif que le signalement s'est avéré, in fine, inexact ou infondé.

La motivation personnelle du lanceur d'alerte et son intérêt personnel ne doivent pas être pris en compte. Ce qui importe lors de l'appréciation de la protection du lanceur d'alerte, ce n'est pas sa motivation, mais bien « la pertinence et l'intérêt de l'information remontée ».

Le lanceur d'alerte qui n'aurait pas agi de bonne foi perd les droits et protections auxquels il aurait pu prétendre et peut faire l'objet de **mesures disciplinaires et de poursuites civiles et/ou pénales**.

### LES PERSONNES LIÉES AUX LANCEURS D'ALERTE

Certaines personnes (physiques ou morales) – qui ne sont pas des lanceurs d'alerte - risquent également de faire l'objet de représailles, par ricochet, de sorte qu'ils vont également pouvoir bénéficier de la protection offerte à ces derniers :

- les facilitateurs : Il s'agit des personnes qui, sans être « lanceurs d'alerte », assistent ou aident l'auteur du signalement à effectuer celui-ci ou lui apportent leur aide dans le cadre de l'enquête et qui risquent, à ce titre, de faire également l'objet de représailles de sorte qu'ils vont également pouvoir bénéficier de la protection offerte à ces derniers ;
- les tiers qui ne participent pas activement au signalement mais sont en lien avec les lanceurs d'alerte, plus spécifiquement, il peut s'agir de collègues ou de proches des lanceurs d'alerte qui travaillent ou ont travaillé dans une autre organisation avec laquelle le lanceur d'alerte est ou a été en contact dans le cadre de son travail ;
- les entités juridiques appartenant aux lanceurs d'alerte ou pour lesquelles ils travaillent, ou encore avec lesquelles ils sont en lien dans un contexte professionnel.

Ces personnes bénéficient des mesures de protection s'ils remplissent, eux aussi, la condition de BONNE FOI, c'est-à-dire s'ils avaient des **motifs raisonnables de croire** que le lanceur d'alerte tombait dans le champ de protection de la présente politique.

## 3.2. QUELLES SONT LES MESURES DE PROTECTION ?

### LA PROTECTION DE L'IDENTITÉ

Le Gestionnaire du signalement est tenu à une **obligation de confidentialité stricte** et utilise des outils sécurisés (accès limités aux e-mails et au disque de stockage, etc…).

L'identité du lanceur d'alerte et de tout facilitateur ou tiers mentionnés dans le signalement est et reste confidentielle durant tout le processus, y compris à l'égard de la hiérarchie de l'auteur, en ce compris les membres des organes de gestion et d'administration et leurs collaborateurs directs. Il en est de même pour tout élément qui pourrait permettre leur identification. En aucun cas, la personne mise en cause dans un signalement ne saurait obtenir des informations sur l'identité de l'auteur du signalement en invoquant son droit d'accès.

Les seules exceptions sont liées aux circonstances suivantes :

- le lanceur d'alerte ou le tiers autorise formellement (consentement exprès et libre) la communication de son identité ;
- la communication de l'identité est strictement nécessaire dans le contexte de l'enquête interne : Il s'agit des personnes déterminées au cas par cas par le Gestionnaire du signalement en fonction des strictes nécessités de l'enquête. Il peut s'agir de collaborateurs du service Compliance ou d'auditeurs internes, ou d'experts techniques ou juridiques, spécialisés dans certaines matières. Ces personnes veillent à ce que les informations reçues soient traitées confidentiellement et respectent les mesures de sécurité.
- Le déclarant pourra demander au Gestionnaire du signalement l'identité de la ou des personne(s) à qui son identité a été communiquée ;
- une enquête ou une procédure judiciaire : L'identité du lanceur d'alerte pourrait aussi devoir être divulguée aux personnes participant à une enquête ou une procédure judiciaire engagée ultérieurement à la suite de l'enquête menée dans le cadre du signalement ;
- une fausse déclaration à des fins malveillantes : Tout abus du système peut aboutir à la perte de la protection légale, ainsi qu'à l'adoption de mesures à l'encontre de l'auteur de cet abus.

### LA PROTECTION CONTRE DES REPRÉSAILLES

Est interdite toute forme de représailles contre les lanceurs d'alerte et contre les personnes qui les ont aidés, en ce compris les menaces de représailles et tentatives de représailles dont : suspension, licenciement, rétrogradation ou refus de promotion, harcèlement etc.

Le cas échéant, toute personne protégée peut adresser une **plainte motivée au coordinateur fédéral**, qui engagera une procédure extrajudiciaire de protection.

Si le lanceur d'alerte estime être victime de représailles, il appartient à Ethias d'établir qu'il ne s'agit pas de mesures de représailles prises suite au signalement à l'égard du lanceur d'alerte qui en subit un dommage.

## 3.3. MESURES DE SOUTIEN

Le lanceur d'alerte a accès à l'Institut fédéral pour la protection et la promotion des droits de l'Homme (FIRM) afin de lui apporter le soutien adéquat, notamment : informations et conseils, facilement accessibles au public et gratuits, sur les procédures et recours disponibles, sur la 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,etc.

## 3.4. EXONÉRATION DE LA RESPONSABILITÉ PÉNALE

Si le lanceur d'alerte a été contraint d'enfreindre une disposition légale, règlementaire ou administrative (expl secret professionnel, ...) pour obtenir ou divulguer les informations relatives au signalement, il ne sera pas poursuivi pour cette infraction si la violation signalée rentre dans les conditions de la protection.

Cette exonération sera maintenue même si l'enquête fait apparaître que le signalement n'était pas fondé, pour autant qu'il ait été effectué de bonne foi.

# 4. MESURES DE PROTECTION DES PERSONNES CONCERNÉES

## 4.1. CONFIDENTIALITÉ

Ethias veille à ce que l'identité des personnes concernées par les signalements soit protégée aussi longtemps que les enquêtes déclenchées par le signalement ou la divulgation publique sont en cours.

## 4.2. INDEMNISATION

En cas de signalement fondé sciemment sur de fausses informations, les personnes concernées victimes de dommages en résultant ont le droit d'obtenir une indemnisation conformément à la responsabilité contractuelle ou extracontractuelle.

# 5. SIGNALEMENT INTERNE VS SIGNALEMENT EXTERNE

Désormais, le lanceur d'alerte a le droit de « choisir le canal de signalement le plus approprié en fonction des circonstances particulières de l'affaire », eu égard à la nature de la violation faisant l'objet du signalement et aux craintes d'éventuelles représailles.

Néanmoins,**il convient de privilégier la voie interne** qui semble être le meilleur moyen pour que l'information parvienne aux personnes qui peuvent contribuer à la résolution rapide et efficace des risques pour l'intérêt public et le plus à même de garantir un équilibre entre les différents intérêts en présence.

## 5.1. DISPOSITIF D'ALERTE INTERNE EN PRATIQUE

### ENVISAGER ET CHOISIR SON CANAL DE SIGNALEMENT

Afin de privilégier un dialogue ouvert et constructif, lorsque vous avez des questions ou préoccupations quant au respect des règles de l'entreprise, ou lorsque vous ne savez pas précisément comment vous devez aborder une situation particulière, il vous est conseillé d'en parler avec votre responsable direct ou à un niveau hiérarchique supérieur ou avec le responsable des Ressources Humaines.

Il est rappelé que, lorsqu'un canal spécifique existe pour remonter et traiter certaines questions précises, les collaborateurs sont invités à utiliser ces canaux en priorité, par exemple : harcèlement moral/sexuel ⇢ Personnes de confiance / Comité pour la prévention et la protection au travail ; etc.

Au cas où ce ne serait pas possible, pour quelle que raison que ce soit, vous pouvez vous adresser au Head of Compliance en tant que responsable de la gestion des signalements internes.

### QUE DOIT CONTENIR LE SIGNALEMENT

Il convient, dans le chef du lanceur d'alerte, de fournir un maximum d'informations, y compris les soupçons raisonnables et les éventuelles preuves matérielles 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.

Ces informations doivent permettre au Head of Compliance de prendre un jugement adéquat sur le fondement, l'étendue et l'urgence de la situation.

Particulièrement dans le cas d'un signalement anonyme par courrier (au vu de l'impossibilité corrélative à communiquer avec un lanceur d'alerte anonyme), les informations reçues doivent être suffisamment complètes, concrètes et claires pour étayer le dossier. Par ailleurs, le Head of Compliance doit pouvoir en déduire que la déclaration a été faite de bonne foi.

### TRAITEMENT ET SUIVI DU SIGNALEMENT INTERNE

Le Head of Compliance qui reçoit un signalement interne , quel que soit le moyen utilisé (bouton « Whistleblower », e-mail, lettre, ...) et qu'elle soit anonyme ou non, doit prendre en charge le signalement, conformément à la procédure expliquée ci-dessous ou il peut désigner un gestionnaire de signalement au sein de son service – et qui doit également avoir la qualité de Compliance Officer – afin de gérer le traitement et le suivi du signalement interne.

## Suivi diligent et approprié du signalement interne

Le lanceur d'alerte est informé par le gestionnaire de signalement de ses droits, obligations et protection, ainsi que du déroulement de la procédure lorsque c'est possible. Il insiste tout particulièrement sur l'exigence de confidentialité et la nécessité d'agir de bonne foi.

Le gestionnaire de signalement effectue une **analyse préliminaire**, laquelle consiste à examiner attentivement chaque signalement interne pour évaluer si elle est admissible, crédible et sérieuse.

Il évalue l'exactitude des allégations formulées dans le signalement et procède, si le dossier le requiert, aux investigations qu'il juge utiles afin d'établir le bien-fondé du signalement et, s'il y a lieu, analyse le dysfonctionnement ou non-respect de règles internes ou externes avéré. Il détermine s'il y a lieu de lancer une enquête interne, des poursuites, une action en recouvrement de fonds, ou de classer sans suite.

Dans certaines circonstances, le lanceur d'alerte (si pas anonyme par courrier) ou certains membres du personnel peuvent être contactés pour recueillir des informations supplémentaires qui permettent de clarifier les allégations formulées. En outre, des recherches discrètes visant à collecter des informations contextuelles, sans alerter un suspect potentiel devraient être lancées.

L'analyse préliminaire d'un signalement, ainsi que toute mesure prise par le gestionnaire de signalement dans ce cadre (mesures telles que : enquête interne, poursuites, actions en recouvrement de fonds ou clôture de la procédure), doit être systématiquement documentée, y compris la description de l'allégation, les étapes prises pour obtenir une compréhension approfondie de l'affaire, la liste des personnes contactées, la documentation consultée ou recueillie et la recommandation d'enquêter ou non sur la question.

Lorsqu'une **enquête détaillée** doit être déclenchée, le gestionnaire de signalement définit l'approche la plus appropriée et détermine qui, au sein de l'entité, doit être informé de manière opportune quant aux allégations et ce, avant que tout devoir d'enquête ne soit mis en œuvre.

Dans ce contexte, il peut requérir l'aide de tout collaborateur de l'entreprise pour atteindre les objectifs énoncés ci-dessus et s'appuiera sur les « personnes autorisées ». Il s'agit des personnes spécifiquement chargées de l'enquête consécutivement au signalement ou de l'adoption des mesures nécessaires dans le cadre du contrôle des faits signalés. Ces personnes seront déterminées au cas par cas, en fonction des strictes nécessités de l'enquête. Il peut s'agir de collaborateurs du service Compliance ou de l'audit interne, d'experts techniques ou juridiques, spécialisés dans certaines matières. Ces personnes veillent à ce que les informations reçues soient traitées confidentiellement et respectent les mesures de sécurité ad hoc.

Dans le délai de trois mois suivant l'accusé de réception du signalement, l'enquête préliminaire doit être terminée et, si l'état du dossier le permet, **le gestionnaire de signalement** en communique les éléments au(x) membres(s) du management concerné(s) pour suite utile. Dans la négative, il poursuivra ses investigations et en informera le Chief Executive Officer.

## Information au lanceur d'alerte interne

Si le lanceur d'alerte n'est pas anonyme, le Gestionnaire de signalement lui fournit :

- un accusé de réception dans un **délai de sept jours** à compter de la réception du signalement ;
- un retour d'informations dans un **délai de trois mois** suivant l'accusé de réception du signalement, sur **(1)** la mesure envisagée ou prise à titre de suivi, **(2)** les motifs du choix de ce suivi : par exemple le renvoi vers d'autres canaux, la clôture de la procédure en raison de preuves insuffisantes ou du classement sans suite car le signalement ne rentrait pas dans le champ d'application de la présente procédure, l'ouverture d'une enquête interne et, éventuellement ses conclusions, ...

## Information à la personne sur qui porte le signalement interne

Ethias doit, dès l'enregistrement des données, informer cette personne de ce que des données personnelles la concernant sont collectées non directement auprès d'elle, des finalités du traitement pour lesquelles les données sont destinées, des faits dont elle est accusée, des directions ou services qui pourraient recevoir le signalement, de la manière d'exercer ses droits d'accès, de rectification et de suppression, et lui communiquer toute information supplémentaire nécessaire pour lui un traitement loyal des données.

### EXCEPTION

S'il existe un risque sérieux que l'enquête sur les faits allégués ou la collecte des preuves nécessaires soit compromise, ou que les preuves puissent être détruites ou modifiées par la personne mise en cause, l'information de cette dernière peut être retardée aussi longtemps que le risque existe.

## Information au Management

Pendant toute la durée de traitement du signalement, ainsi que pendant l'enquête, le Head Compliance Officer fait régulièrement le point avec le CEO.

Par ailleurs, les recommandations du Head Compliance Officer sont soumises au Management pour décision.

# REGISTRE DES SIGNALEMENTS INTERNES

Le Head of Compliance tient un registre répertoriant tous les signalements internes reçus.

Ce registre mentionne : la date de réception du signalement, le canal utilisé, le destinataire initial, la catégorie du signalement interne , la description désintéressée de l'affaire (**aucun nom ne doit être fourni dans cette section** - seulement le nom du département), une description sommaire de ce qui a été fait et des principales constatations factuelles, le statut de l'affaire, la date d'achèvement de l'enquête, une indication des prochaines étapes (mesures correctives, sanctions disciplinaires, procédure judiciaire) et la suite qui y a été donnée ou la raison pour laquelle il n'a pas été jugé nécessaire d'y donner suite (par exemple, le motif pour lequel le signalement a été estimé non fondé).

Le registre des signalements doit être mis à jour corrélativement au suivi de chaque signalement interne (ex: fermé, sous enquête).

Chaque signalement interne reçoit un numéro de référence séquentiel unique et ne sera pas conservée plus longtemps que nécessaire.

## 5.2. SIGNALEMENT EXTERNE : DÉCLENCHÉ EN DEHORS D'ETHIAS

### SIGNALEMENT À LA BNB

La BNB a mis en place un dispositif de signalement externe en vertu duquel toute personne peut signaler « tout manquement et infraction potentiel ou avéré aux dispositions des lois belges et règlements européens, en ce compris de toutes dispositions réglementaires prises pour leur application, relatives au statut et au contrôle des établissements financiers et à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, dont la BNB a pour mission d'assurer le contrôle ».

Le signalement se fait via un formulaire disponible sur son site Internet :

www.nbb.be/fr/supervisionfinanciere/generalites/signaler-uneinfraction/formulaire-de-signalement-duneinfraction

### SIGNALEMENT À LA FSMA

La procédure de signalement externe auprès de la FSMA et les règles de protection des informateurs sont similaires à celles applicables à la BNB dans la mesure où elles les ont inspirées. Par ailleurs, la FSMA a lancé en 2017 le « Point de Contact Lanceurs d'alerte » en ligne afin de permettre aux lanceurs d'alerte de lui signaler les infractions à la législation financière dont elle contrôle le respect.

### SIGNALEMENT AU COORDINATEUR FÉDÉRAL

Le lanceur d'alerte externe peut également s'adresser au Coordinateur fédéral chargé de réceptionner les signalements externes, examiner leur recevabilité et orienter l'auteur de signalement vers les autorités compétentes.

# 6. TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

Tout traitement de données à caractère personnel effectué en vertu de la présente procédure est effectué conformément aux exigences du GDPR, ainsi qu'à notre Politique interne de Protection des données.

Les données à caractère personnel qui ne sont manifestement pas pertinentes pour le traitement d'un signalement spécifique ne sont pas collectées ou, si elles le sont accidentellement, sont effacées sans retard injustifié.

Le nom, la fonction et les coordonnées du lanceur d'alerte de signalement, ainsi que de toute personne à qui les mesures de protection et de soutien s'étendent, sont sauvegardés jusqu'à ce que la violation signalée soit prescrite.

ethias