

DISPOSITIF D'ALERTE INTERNE

L'engagement de la direction

Le dispositif d'alerte interne de SMI permet à chacun, parties prenantes internes et externes, notamment les collaborateurs et les partenaires commerciaux, de signaler de manière sereine de potentielles violations de la réglementation ou des pratiques susceptibles d'être contraires à l'éthique.

Ce dispositif est un moyen efficace pour détecter les situations présentant des risques pour l'entreprise et renforcer notre culture de l'intégrité.

SMI garantit un traitement confidentiel des signalements et assure la protection de leurs auteurs qui agissent de bonne foi, contre toute forme de représailles.

L'efficacité de ce dispositif d'alerte repose sur sa diffusion mais également sur sa bonne compréhension par les personnes susceptibles d'y avoir recours : c'est l'objectif de cette procédure dont la vocation est d'expliquer de manière claire ses objectifs et son fonctionnement.

Je sais pouvoir compter sur l'ensemble des collaborateurs pour utiliser le dispositif d'alerte de façon responsable afin de nous permettre d'identifier les sujets sur lesquels SMI peut s'améliorer.

Bertrand Da Ros

SOMMAIRE

Préambule	3
I. La protection du lanceur d'alerte	7
1. Les conditions permettant de bénéficier de la protection légale	7
2. Les protections prévues par la loi	7
II. Le dispositif d'alerte interne de SMI	9
III. La prévention et la gestion des conflits d'intérêts dans le traitement des signalements	11
IV. Le recueil des signalements	12
1. La publicité sur le dispositif d'alerte interne	12
2. L'accès à la plateforme d'alerte	12
3. La déclaration d'un signalement	12
4. L'accusé de réception	13
5. Les notifications	14
6. Les garanties de confidentialité	14
V. Le traitement des signalements	15
1. L'analyse de recevabilité du signalement	15
2. Les investigations	16
3. Les décisions prises à l'issue des investigations	16
4. La clôture du signalement	17
VI. Le reporting sur le dispositif d'alerte interne	19
VII. La politique de protection des données personnelles	20
Glossaire	23

Préambule

Cadre légal

1. Le dispositif d'alerte interne de SMI s'appuie sur **les principes et obligations issus de la loi Sapin 2¹** qui instaure **un régime protecteur des lanceurs d'alerte**.

2. Cette protection a été renforcée par la loi « Waserman » du 21 mars 2022 et son décret d'application² qui comportent les principales modifications suivantes :

- la possibilité pour toute partie prenante externe d'effectuer un signalement auprès de l'entreprise (candidat à un emploi, ancien collaborateur, sous-traitant, fournisseur, client, etc.) ;
- la possibilité de faire un signalement directement auprès de l'autorité compétente ;
- le renforcement de la protection des lanceurs d'alerte, en particulier contre les mesures de représailles, ainsi qu'une nouvelle protection des personnes qui les aident ;
- la possibilité de signaler des faits dont la personne n'a pas nécessairement eu personnellement connaissance, si les informations ont été obtenues dans un cadre professionnel.

La présente procédure d'alerte intègre ces évolutions réglementaires.

3. Le dispositif d'alerte interne SMI répond également à l'obligation de déployer :

- un dispositif permettant de signaler toute conduite ou situation contraire au code de conduite anticorruption SMI au titre du **dispositif anticorruption³** ;
- un mécanisme d'alerte permettant de signaler tout risque d'impacts négatifs réels ou potentiels associés aux activités du groupe Covéa ou à ses relations d'affaires au titre du **devoir de vigilance⁴**.

4. Le dispositif d'alerte interne permet aux personnes auxquelles il est ouvert de signaler à SMI des faits entrant dans son champ d'application et d'assurer un traitement efficace et confidentiel des signalements reçus.

Il repose sur des principes de bonne foi, de loyauté ainsi que sur le respect des droits de la défense

5. L'utilisation du dispositif d'alerte interne et de la plateforme dédiée est facultative : c'est un canal de signalement parmi d'autres, notamment pour les collaborateurs qui disposent d'autres moyens : la voie hiérarchique, le responsable des ressources humaines, les représentants du personnel.

Ainsi, le fait de ne pas utiliser ce dispositif ne peut entraîner aucune sanction à leur rencontre.

Toutefois, le dispositif d'alerte interne peut être plus approprié en fonction de la situation.

De plus, il permet de bénéficier de la protection liée au statut de lanceur d'alerte et d'une confidentialité renforcée.

¹ Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique (art. 6 et s.).

² Décret n° 2022-1284 du 3 octobre 2022 relatif aux procédures de recueil et de traitement des signalements émis par les lanceurs d'alerte et fixant la liste des autorités externes instituées par la loi n°222-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte.

³ Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique (art. 17-II 3).

⁴ Loi n° 2017-399 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre qui vise à prévenir les atteintes graves envers les droits humains et les libertés fondamentales, la santé et la sécurité des personnes ainsi que l'environnement

6. Le dispositif d’alerte ne se substitue pas à la possibilité offerte par la loi au lanceur d’alerte de saisir directement ou à tout moment les **autorités compétentes**⁵.

7. L’utilisation du dispositif d’alerte est un droit pour les collaborateurs. Par conséquent, aucun collaborateur ne peut subir de représailles ou de sanction disciplinaire pour avoir relaté des faits ou témoigné de bonne foi dans le cadre du dispositif d’alerte, même si les faits allégués dans le signalement s’avèrent finalement infondés ou inexacts et ne donnent lieu à aucune suite.

En revanche, l’utilisation abusive ou de mauvaise foi du dispositif d’alerte peut exposer son auteur à des sanctions disciplinaires ainsi qu’à des poursuites judiciaires.

La mauvaise foi consiste par exemple à utiliser le dispositif pour dénoncer des faits dont la personne sait qu’ils sont faux ou porter des allégations diffamatoires à l’encontre d’une tierce personne, avec l’intention de nuire ou encore dans l’espoir d’en retirer une contrepartie indue.

8. Le dispositif d’alerte interne SMI a fait l’objet d’une information et d’une consultation des instances représentatives du personnel, conformément aux dispositions légales.

Information sur la possibilité d’effectuer un signalement externe

Il est possible, directement ou après avoir effectué un signalement interne, d’adresser son signalement externe aux autorités compétentes :

- l’autorité judiciaire ;
- l’autorité compétente parmi celles mentionnées dans le décret ;
- le Défenseur des droits, afin d’être orienté vers l’autorité la plus à même de traiter le signalement ;
- éventuellement une institution, un organe ou un organisme de l’Union européenne compétent.

Zoom sur le choix de la procédure de signalement

Il est possible de choisir le canal qui semble le plus approprié, notamment en termes de traitement efficace, impartial et confidentiel du signalement :

- le signalement interne consiste à s’adresser à l’entreprise concernée par les faits ;
- le signalement externe consiste à s’adresser à l’autorité compétente (autorité judiciaire pour une infraction, autorité administrative).

En cas de difficulté pour identifier l’autorité compétente, le Défenseur des droits peut être sollicité pour orienter vers l’autorité compétente.

À savoir

Dans des cas très spécifiques et encadrés par la loi, il est possible de divulguer publiquement son signalement. Ces conditions étant très restrictives, il est conseillé de se rapprocher du Défenseur des droits avant d’actionner la divulgation publique.

⁵ Liste disponible dans l’annexe du décret n°2022-1284 du 3 octobre 2022 relatif aux procédures de recueil et de traitement des signalements émis par les lanceurs d’alerte et fixant la liste des autorités externes instituées par la loi n° 222-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d’alerte.

Champ d'application

1. Les faits pouvant faire l'objet d'un signalement doivent être répréhensibles ou contraires à l'intérêt général :

- un crime ou un délit ;
- une menace ou un préjudice pour l'intérêt général ;
- une violation ou une tentative de dissimulation d'une violation des lois et règlements nationaux, européens ou internationaux ;
- des manquements ou des situations contraires au code de conduite anticorruption de SMI ;
- des risques d'atteintes aux droits humains, libertés fondamentales, santé, sécurité des personnes et à l'environnement⁶.

Exception

En France, sont exclues du régime de l'alerte les informations, quels que soient leur forme ou leur support, couvertes par :

- le secret de la défense nationale ;
- le secret médical ;
- le secret de l'enquête ou de l'instruction judiciaire ;
- le secret professionnel de l'avocat.

Seuls les faits présentant un caractère **illicite** ou portant **atteinte à l'intérêt général** en lien avec les activités de l'entreprise peuvent faire l'objet d'un signalement.

Ainsi, ne peuvent pas fonder un signalement :

- un simple dysfonctionnement interne à l'entreprise ;
- un **mécontentement** lié à la relation avec SMI ; y compris une insatisfaction des collaborateurs à l'égard de l'évaluation de leur performance ou du déroulement de leur carrière, sauf en cas de manquement à la réglementation ;
- une **infraction commise par un tiers** n'agissant pas pour le compte de SMI ;
- les **réclamations commerciales** usuelles doivent être adressées au service réclamation compétent ;
- les **remontées d'alertes** sur les opérations ou situations atypiques de la clientèle au titre de la lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT) doivent être déclarées auprès du correspondant/déclarant Tracfin.

2. Le présent dispositif d'alerte est ouvert notamment :

- aux collaborateurs de SMI, quel que soit leur statut⁷ ;
- aux collaborateurs externes ou occasionnels⁸ ;
- aux anciens salariés et candidats à l'embauche ;
- aux titulaires de droits de vote aux assemblées générales (membres participants) ;
- aux membres des organes de gouvernance de SMI ;
- aux cocontractants de SMI et à leurs sous-traitants ;
- et plus largement aux parties prenantes externes de l'entreprise.

⁶ Illustrations des atteintes graves pouvant faire l'objet d'un signalement au titre du devoir de vigilance :

- atteinte à l'égalité, au respect de la vie privée, au droit de grève, à la liberté de réunion ou d'association ;
- risque sanitaire, non-respect des conditions de travail légales.

⁷ CDI, CDD, alternants, stagiaires.

⁸ Intérimaires, prestataires.

Interlocuteurs

1. Les collaborateurs de SMI peuvent se rapprocher de leurs interlocuteurs habituels :

- le manager ;
- le directeur des ressources humaines.

2. Ils peuvent également saisir le **responsable conformité** à l'adresse suivante ethique@mutuelle-smi.com afin d'obtenir un conseil, préalablement à l'utilisation du dispositif d'alerte interne.

Dans ce cas, la personne ne bénéficie pas de la protection du lanceur d'alerte.

I. La protection du lanceur d'alerte

1. Les conditions permettant de bénéficier de la protection légale

Afin de bénéficier de la protection du lanceur d'alerte, il est nécessaire de remplir l'ensemble des conditions suivantes :

1. être une personne physique : les personnes morales ne sont pas considérées comme des lanceurs d'alerte ;
2. ne retirer aucune contrepartie financière directe du fait du signalement (une rémunération, une prime ou une augmentation) ;
3. être de bonne foi : il faut avoir des motifs raisonnables de croire que les faits signalés sont véridiques ;
4. signaler des faits relevant du dispositif d'alerte (faits illicites ou portant atteinte à l'intérêt général) ;
5. si les informations signalées ont été obtenues en dehors du contexte professionnel, il est nécessaire d'avoir eu personnellement connaissance de ces faits.

A contrario, cette condition relative à la connaissance personnelle des faits n'est pas nécessaire pour obtenir le statut de lanceur d'alerte lorsque l'information a été obtenue à l'occasion d'une activité professionnelle.

2. Les protections prévues par la loi.

Si l'auteur d'un signalement remplit toutes les conditions pour être reconnu lanceur d'alerte, il peut bénéficier des protections suivantes :

1. le statut protecteur de lanceur d'alerte est d'ordre public, ce qui signifie qu'il n'est pas possible d'y renoncer par quelque moyen que ce soit ;
2. la confidentialité de l'identité du lanceur d'alerte doit être assurée par les personnes qui recueillent et traitent les signalements. Le manquement à cette obligation est passible d'une sanction pénale de deux ans d'emprisonnement et de 30 000 euros d'amende.

Exception

Les éléments de nature à identifier le lanceur d'alerte peuvent être communiqués à l'autorité judiciaire si l'entreprise a l'obligation de signaler les faits à celle-ci. Le lanceur d'alerte est informé de cette communication sauf dans l'hypothèse où cette information risque de compromettre la procédure judiciaire.

3. En tant que salarié, le lanceur d'alerte ne peut pas être sanctionné par son employeur⁹ ni subir des mesures de représailles du fait de son signalement. Le code du travail liste 15 mesures interdites à son encontre (sanctions disciplinaires, mutation, évaluation de la performance négative, etc.).
4. En cas de mesures négatives prises à son encontre, le lanceur d'alerte peut saisir le conseil des prud'hommes en référé. Il peut également obtenir indemnisation de son préjudice (perte de rémunération à la suite du signalement).

⁹ Cf article L1132-3-3 du code du travail ¹⁰ CDI, CDD, alternants, stagiaires.

Il appartient à l'employeur de prouver que les mesures prises à son égard n'ont aucun lien avec le signalement.

5. Par ailleurs, la loi prévoit :

- une absence de responsabilité civile du lanceur d'alerte si son signalement apparaît nécessaire à la sauvegarde des intérêts en cause et respecte les règles prévues par les textes ;
- une absence de responsabilité pénale du lanceur d'alerte en cas de délit de divulgation d'une information confidentielle ou d'un secret dont il a eu connaissance de manière licite, par exemple, dans le cadre du poste occupé.

La divulgation de ces informations doit toutefois être nécessaire et proportionnée à la sauvegarde des intérêts en cause.

6. Le lanceur d'alerte peut bénéficier :

- d'un soutien financier décidé par le juge saisi (frais d'instance ou subsides si sa situation financière s'est dégradée) au cours d'une procédure judiciaire ;
- de mesures favorisant sa réinsertion professionnelle :
 - le référé prud'homal permet au juge de se prononcer rapidement sur le licenciement ;
 - le juge peut imposer à l'employeur d'abonder le compte personnel de formation du lanceur d'alerte ;
- de mesures de soutien psychologique et financier par l'autorité externe compétente.

7. La loi prévoit des sanctions à l'encontre des auteurs de représailles ou en cas de « **procédures baillons**¹⁰ », notamment :

- le fait d'empêcher une personne de faire un signalement est un délit sanctionné d'un an d'emprisonnement et de 15 000 euros d'amende ;
- le fait d'engager un recours abusif contre un lanceur d'alerte est sanctionné d'une amende civile pouvant atteindre 60 000 euros.

8. La protection est élargie à l'entourage des lanceurs d'alertes :

- les « facilitateurs », c'est-à-dire les personnes physiques pouvant risquer des mesures de représailles (un collègue) ou les personnes morales de droit privé à but non lucratif (association, syndicat, organisation non gouvernementale) qui soutiennent le lanceur d'alerte ;
- les personnes en lien avec le lanceur d'alerte (collègue, proche, sous-traitant de l'employeur) et l'entité juridique en lien avec le lanceur d'alerte (une société contrôlée par lui ou pour laquelle il travaille).

¹⁰ Par exemple, une action en justice en diffamation pour intimider le lanceur d'alerte.

II. Le dispositif d'alerte interne de SMI

1. Le dispositif d'alerte interne de SMI repose sur :

- la **présente procédure** qui détaille :
 - les conditions permettant de bénéficier de la protection du statut de lanceur d'alerte ;
 - le processus de gestion des signalements ;
- une **plateforme sécurisée** permettant le recueil et le traitement des signalements dans des conditions assurant sécurité et confidentialité ;
- une **organisation avec des acteurs identifiés**, détaillés dans le tableau ci-dessous. Ces personnes, en nombre restreint, sont choisies en raison de leurs compétences respectives, nécessaires pour traiter les signalements.

ACTEUR	MISSION
Référent alertes	<p>Il s'agit du responsable conformité désigné par le directeur général de SMI pour recueillir et traiter les signalements.</p> <p>Il est garant du bon fonctionnement de l'ensemble du dispositif d'alerte interne et préside le comité d'éthique.</p>
Comité d'éthique	<p>Ce comité est chargé d'épauler le référent alertes pour :</p> <ul style="list-style-type: none">▪ l'analyse des signalements reçus ;▪ la conduite des investigations ;▪ la prise de décision sur les suites à donner. <p>Il est constitué de membres permanents en nombre restreint : directeur général (DG) – directeur des ressources humaines (DRH) – responsable conformité.</p> <p>Le cas échéant, en fonction de l'objet et du contexte du signalement, d'autres directeurs peuvent y participer. Ce comité permet d'assurer une collégialité dans la prise de décision.</p>
Cellule d'investigation	<p>Elle est composée du DRH et du responsable conformité.</p> <p>En fonction du sujet de chaque signalement, les collaborateurs compétents sont missionnés pour procéder aux investigations visant à établir la véracité des faits signalés.</p>
Instance dirigeante	<p>L'instance dirigeante est informée par le référent alertes des enquêtes internes relatives aux situations les plus sensibles (notamment d'éventuelles infractions pénales), à l'exception de celle où elle est elle-même mise en cause.</p> <p>Cette information est assurée de telle manière qu'elle préserve la confidentialité de l'identité de l'auteur du signalement.</p>

2. L'ensemble de ces personnes est assujéti à une clause de confidentialité spécifique qui rappelle la sanction pénale encourue en cas de divulgation de l'identité du lanceur d'alerte.

- 3.** En fonction du contexte du dossier, le comité d'éthique peut décider de confier les investigations :
- soit en interne aux membres compétents de la cellule d'investigation ;
 - soit en externe à tout tiers autorisé, en raison de ses compétences et/ou de son impartialité ou encore en raison de la complexité ou de la sensibilité de l'enquête.

Il peut s'agir d'avocats, d'experts, d'auditeurs, sous réserve qu'ils soient assujettis par la loi ou un contrat à une obligation de confidentialité renforcée.

III. Le dispositif d'alerte interne de SMI

1. Les membres du comité d'éthique disposent de moyens leur permettant d'exercer leur mission de manière impartiale et autonome.

Ils sont sensibilisés aux principales dispositions réglementaires encadrant le recueil et le traitement des signalements.

2. Les membres du comité d'éthique et l'ensemble des personnes participant au recueil et au traitement des signalements s'engagent à ne pas agir en cas de conflit d'intérêts.

Ainsi, **ils doivent déclarer toute situation de conflit d'intérêts** potentiel, apparent ou avéré du fait des liens qu'elles entretiennent avec un protagoniste du signalement (auteur, témoin, victime, personne mise en cause) ou de leur responsabilité dans le processus mis en cause par le signalement. Cette obligation consiste à déclarer par écrit au référent alertes le conflit d'intérêts en question, **avant toute participation au traitement de l'alerte ou, à défaut, dès lors que le conflit d'intérêts apparaît au cours de l'enquête.**

3. La situation de conflit d'intérêts est alors analysée par le responsable conformité puis présentée au comité d'éthique avec une proposition de mesure de remédiation, le cas échéant. Si le conflit d'intérêts est confirmé, le comité d'éthique valide la mesure de remédiation afin de faire cesser la situation de conflit d'intérêts.

Il peut notamment s'agir d'un départ et du remplacement du titulaire par son suppléant ou de l'externalisation des investigations.

Cette mesure sera formalisée par écrit par le référent alertes qui en informera la personne concernée.

4. Si le référent alertes est lui-même en situation de conflit d'intérêts, le comité d'éthique décide d'externaliser la conduite des investigations.

La décision prise est formalisée par écrit et diffusée au à l'instance dirigeante.

IV. Le recueil des signalements

1. La publicité sur le dispositif d'alerte interne

1. La connaissance du dispositif d'alerte de SMI par les collaborateurs et les parties prenantes externes est indispensable à son efficacité.
2. L'ensemble du personnel SMI est informé de l'existence du dispositif et de la présente procédure grâce à des communications internes et à la présentation du dispositif dans l'intranet le cas échéant.
3. Les tiers sont informés de l'existence du dispositif grâce à des informations sur le site institutionnel : <https://www.mutuelle-smi.com/qui-sommes-nous/nos-engagements/>.

2. L'accès à la plateforme d'alerte

1. La confidentialité des signalements et la protection de leur auteur sont des préoccupations fondamentales pour SMI.

C'est la raison pour laquelle les signalements sont recueillis et traités grâce à une plateforme sécurisée qui offre un espace d'échanges cryptés, déconnecté des systèmes d'information de l'entreprise et ne permettant pas la traçabilité des adresses IP.

Seules les personnes habilitées peuvent accéder aux signalements.

2. Cette plateforme externe est :
 - disponible en permanence ;
 - disponible en langue française ;
 - accessible de n'importe quel appareil connecté à internet (ordinateur, tablette, smartphone).
3. La plateforme d'alerte est facilement accessible.

Pour les collaborateurs :

- à partir des applications de l'intranet SMI.

Pour les tiers :

- soit sur le site institutionnel de SMI : <https://www.mutuelle-smi.com/qui-sommes-nous/nos-engagements/>
- soit en utilisant l'adresse URL : <https://covea.whispli.com/smi>.

3. La déclaration d'un signalement

1. Avant de faire son signalement dans un formulaire en ligne, le déclarant est invité à créer un compte lui permettant de déclarer son signalement puis de consulter la plateforme ultérieurement pour échanger avec le référent alertes et pour suivre le traitement de son signalement.

Le déclarant a également la possibilité de se connecter sans créer de compte, avec un profil « Invité ».

Le déclarant a aussi la possibilité d'effectuer un signalement anonyme.

2. Le déclarant doit prendre connaissance de la présente procédure avant de faire sa déclaration afin de **s'assurer que les faits qu'il souhaite signaler entrent bien dans le présent dispositif**. À défaut, il est invité à utiliser les autres dispositifs existants ou à solliciter le responsable conformité (ethique@mutuelle-smi.com) afin d'être aiguillé sur la bonne procédure.

3. Le déclarant complète ensuite le formulaire en ligne lui demandant de décrire l'objet de son signalement.

Il est invité à communiquer des informations les plus factuelles, précises et exhaustives possibles **en lien direct avec l'objet du signalement** :

- les faits ;
- les personnes impliquées ;
- le lieu et la date ou la période relatifs aux faits signalés.

Les informations communiquées devront porter sur des **faits objectifs, matériellement vérifiables et pertinents** au regard des manquements supposés et en lien direct avec l'objet du signalement.

Ces informations doivent permettre de procéder à une évaluation de la nature, de l'étendue et de l'urgence de la problématique signalée, et doivent être **étayées par des preuves**, si possible écrites.

La formulation des allégations doit faire apparaître le caractère présumé des faits et ne pas porter atteinte à la vie privée des personnes visées.

4. Le déclarant a ensuite le choix de décliner son **identité** ou de **rester anonyme**. Dans ce cas, son attention est attirée sur le fait :

- qu'un signalement anonyme est examiné avec précaution afin d'éviter le risque de signalement malveillant ;
- que les investigations peuvent s'avérer plus fastidieuses ;
- qu'il est alors plus difficile d'assurer son éventuelle protection en tant que lanceur d'alerte puisque son identité n'est pas connue.

À tout moment au cours du traitement du signalement, l'auteur du signalement peut lever l'anonymat.

Si le signalement a été réalisé de manière anonyme et que son auteur n'a pas indiqué d'adresse email pour recevoir les notifications, **il devra se connecter spontanément et régulièrement** à la plateforme pour consulter ses messages et répondre aux demandes d'informations complémentaires.

5. Une fois son formulaire entièrement complété, le déclarant est invité à relire la restitution de sa déclaration avant de la **valider**.

Le cas échéant, les champs obligatoires qui n'ont pas été renseignés sont alors mentionnés afin qu'il puisse compléter sa déclaration.

4. L'accusé de réception

Une fois le formulaire validé et envoyé, un message accusant immédiatement réception du signalement est envoyé sur la messagerie sécurisée.

5. Les notifications

Il est possible de recevoir des notifications afin d'être averti de la réception d'un nouveau message dans la messagerie sécurisée :

- soit par email sur l'adresse mail indiqué lors de la création du compte ;
- soit par notification push dans l'application mobile Whispli que vous aurez téléchargée ;

6. Les garanties de confidentialité

Le dispositif d'alerte de SMI garantit une stricte confidentialité de l'identité de l'auteur du signalement de bonne foi, qu'il bénéficie du statut de lanceur d'alerte (voir conditions supra) ou non, à toutes les étapes du traitement du signalement.

Ainsi :

- le contenu du signalement réalisé en ligne sur la plateforme est crypté de bout en bout¹¹ ;
- tous les échanges sont réalisés sur une messagerie sécurisée hébergée sur la plateforme d'alerte et demeurent confidentiels ;
- les personnes habilitées à recueillir et traiter les signalements sont en nombre restreint et sont assujetties à une obligation spécifique de confidentialité ;
- le cas échéant, les experts missionnés dans le cadre des investigations s'engagent à assurer la confidentialité des données liées au signalement et à les supprimer au terme de leur mission ;
- les informations de nature à identifier le lanceur d'alerte ne sont jamais divulguées aux personnes visées par le signalement : auteur(s) présumé(s) des faits signalés, victime(s) ou témoin(s) ;
- lorsqu'un signalement est réalisé de manière anonyme, la plateforme garantit une poursuite des échanges également de manière anonyme. Aucun procédé¹² ne sera mis en œuvre afin de permettre l'identification de l'auteur du signalement.

¹¹ Cryptage AES-256

¹² Tels que : collecte de l'adresse IP, dépôt de cookies.

V. Le traitement des signalements

1. La phase de traitement des signalements débute avec la réception du signalement sur la plateforme. Elle prend fin par la prise de décision quant aux suites à donner au signalement et par l'information de son auteur et des personnes visées par les faits.

2. L'auteur du signalement est informé à chaque étape du processus grâce à la messagerie sécurisée de la plateforme :

- de la bonne réception de son signalement par un accusé de réception immédiatement après avoir adressé son signalement sur la plateforme ;
- de l'irrecevabilité de son signalement, le cas échéant ;
- de l'état d'avancement du traitement de son signalement dans les trois mois à compter de sa réception (sauf circonstances particulières justifiant un délai plus long) ;
- de la fin des investigations et de la clôture du signalement ainsi que des principales mesures prises pour remédier à la situation, le cas échéant.

1. L'analyse de recevabilité du signalement

1. Les signalements font l'objet d'une analyse de recevabilité afin de déterminer s'ils entrent bien dans le dispositif d'alerte interne et respectent les conditions posées par la loi.

2. Cette analyse, qui peut nécessiter quelques investigations préalables, est réalisée par le référent alertes.

Pendant cette phase, il peut être demandé des informations complémentaires ou des clarifications par des échanges sur la messagerie sécurisée. Dans ce cas, l'auteur du signalement recevra une notification (par e-mail ou sur l'application) l'invitant à se connecter à la plateforme.

S'il n'a pas activé les notifications, il devra se connecter régulièrement à la plateforme.

3. Les conclusions de l'analyse de recevabilité du signalement peuvent être présentées selon les cas au comité d'éthique pour validation.

4. Le comité d'éthique statue sur la recevabilité du signalement et décide des suites à donner :

- si le signalement n'est pas recevable, un message informe l'auteur du signalement de la clôture de son signalement et des raisons de celle-ci. Il peut également être redirigé vers le service compétent pour traiter les faits concernés ;
- si le signalement est recevable, il désigne les personnes chargées de mener les investigations en fonction de la nature et du domaine sur lequel porte le signalement.

5. En cas de signalement anonyme, le référent alertes veille à entourer le traitement de ce signalement de précautions particulières, notamment au moment de son examen préalable de recevabilité, en s'assurant que les faits signalés sont suffisamment crédibles, sérieux et détaillés. Les signalements anonymes considérés comme recevables seront traités de la même manière que les autres, sous réserve que leur auteur réponde aux demandes d'informations complémentaires au cours des investigations dans des délais raisonnables.

Si le signalement a été réalisé de manière anonyme et que son auteur n'a pas indiqué d'adresse e-mail pour recevoir les notifications, il devra se connecter régulièrement à la plateforme pour consulter ses messages et répondre aux demandes d'informations complémentaires.

À défaut et si son signalement ne comporte pas d'informations suffisamment détaillées pour mener des investigations afin d'établir l'exactitude des faits, celui-ci sera clôturé sans suite.

2. Les investigations

1. Les investigations portant sur les signalements recevables sont menées par des personnes habilitées et désignées par le comité d'éthique. Seules les personnes spécifiquement habilitées à les traiter accèdent aux signalements. Le référent alertes et son équipe diligentent ou coordonnent les investigations.

2. L'objectif de ces investigations est de vérifier la matérialité et l'exactitude des faits signalés. La plateforme d'alerte permet de consigner les diligences accomplies pendant toute la durée de l'enquête (analyse juridique et technique des faits, prise de mesures conservatoires collecte de preuves, échanges et/ou entretien avec les parties prenantes, audition de témoins ou de personnes pouvant fournir des informations pertinentes en lien avec les faits, réalisation d'actes d'expertises).

3. Toutes les mesures conservatoires nécessaires sont prises pour préserver les preuves permettant d'établir les faits signalés.

4. Une fois ces mesures prises, une information écrite est assurée par le référent alertes à la personne mise en cause dans le signalement sur le traitement de ses données personnelles au titre du dispositif d'alerte.

5. Les investigations menées peuvent conduire à questionner l'auteur du signalement afin d'obtenir des informations complémentaires ou des précisions nécessaires à l'instruction du signalement, sur la plateforme sécurisée. Il est attendu que l'auteur du signalement réponde dans un délai raisonnable afin de permettre la bonne conduite des investigations.

6. À tout moment et de sa propre initiative, l'auteur du signalement peut transmettre de manière totalement sécurisée, grâce à la plateforme, des informations ou des documents complémentaires permettant d'étayer son signalement dont il a eu connaissance postérieurement à sa déclaration initiale.

7. À l'issue des investigations, la/les personne(s) missionnée(s) peuvent présenter dans un rapport écrit un compte-rendu des opérations de vérifications réalisées, ses/leurs constatations, ses/leurs conclusions ainsi que des propositions de mesures correctives le cas échéant.

8. Dans tous les cas, l'auteur du signalement est informé dans les trois mois à compter de l'accusé de réception de l'avancement du traitement de son signalement. Cette information porte sur :

- les mesures d'investigations réalisées pour établir l'exactitude des faits ;
- et, le cas échéant, les mesures de remédiation mises en œuvre.

3. Les décisions prises à l'issue des investigations

1. Le comité d'éthique décide des suites à donner :

- classement sans suite si les faits ne sont pas avérés, que l'enquête n'établit pas la véracité des faits allégués ou que les preuves collectées sont insuffisantes ;
- signalement avec suites si les faits sont avérés.

Ces suites peuvent être :

- des mesures de remédiation internes, par exemple : renforcement d'un processus, sensibilisation ou formation des collaborateurs concernés, rappel des règles applicables, action de communication ;
- une rupture de la relation contractuelle avec un tiers (si celui-ci est mis en cause) ;
- des mesures disciplinaires ;
- une action en justice.

2. Le comité d'éthique confie alors la gestion du dossier à la direction compétente afin qu'elle prenne en charge les suites à donner.

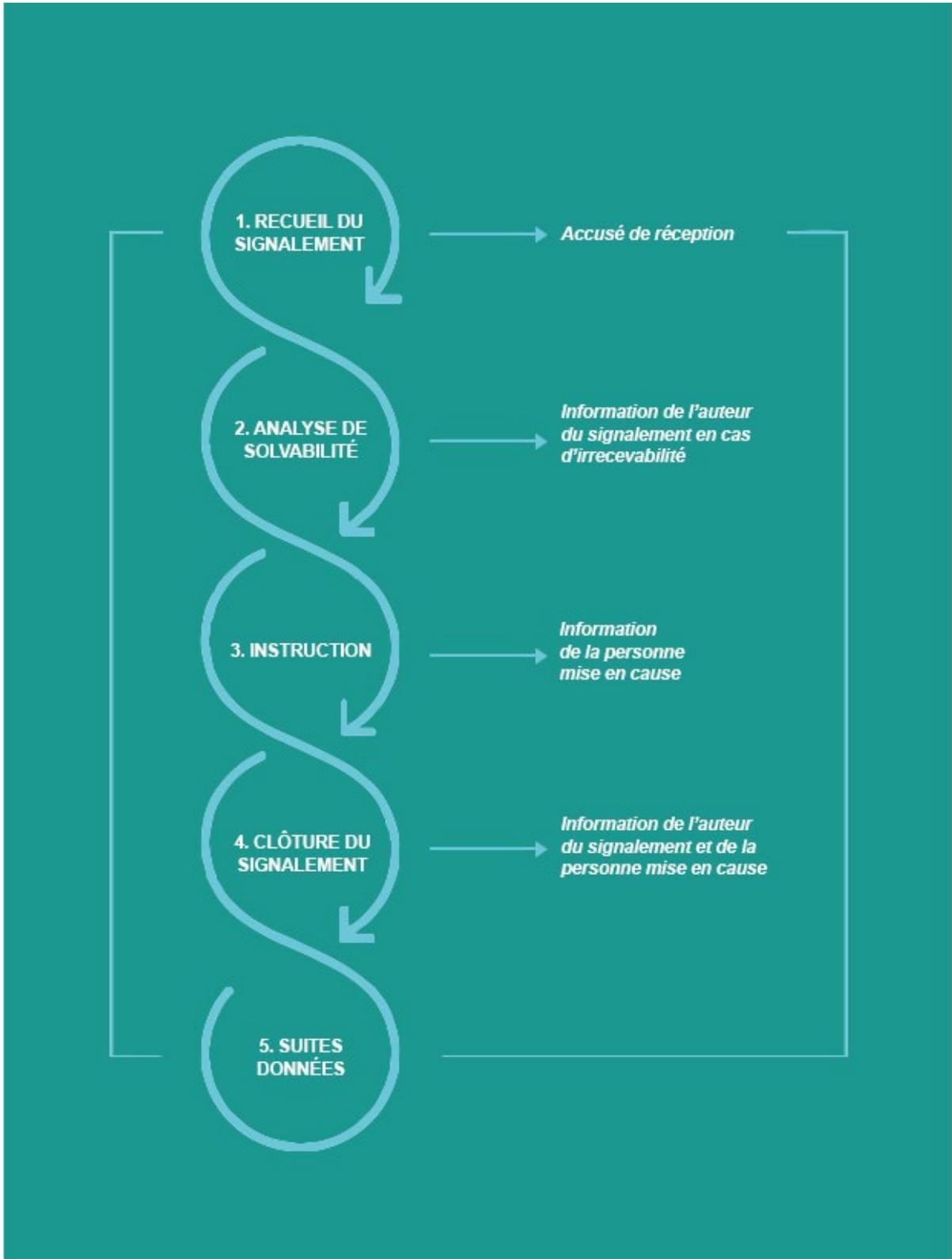
4. La clôture du signalement

1. L'auteur du signalement est informé par écrit de la clôture de son signalement et de la décision prise au terme de l'instruction du dossier.

2. La personne concernée est informée par tout moyen approprié, soit par le référent alertes, soit par un membre du comité d'éthique, des suites données au signalement.

Si un collaborateur est mis en cause au terme des investigations, la direction des ressources humaines l'informe selon la procédure existante.

3. Les données personnelles sont conservées puis anonymisées ou supprimées conformément à la politique de protection des données personnelles détaillée ci-après.



VI. Le reporting sur le dispositif d'alerte interne

Un reporting totalement anonymisé est produit annuellement par le référent alertes qui porte sur l'ensemble des signalements reçus et traités au cours de l'année écoulée.

Ce reporting présente une analyse quantitative et qualitative des données (notamment : typologies des thèmes faisant l'objet de signalements, taux de recevabilité, types de suites données).

Il est présenté annuellement au comité d'éthique ainsi qu'à l'instance dirigeante de SMI.

VII. La politique de protection des données personnelles

1. Par qui les données sont-elles traitées ?

Les données personnelles sont traitées par SMI, responsable du traitement.

2. Quels sont les types de données traitées ?

Les données sont traitées dans le cas où une personne signale des informations portant sur les faits suivants :

- un crime, un délit, une menace ou un préjudice pour l'intérêt général, une violation d'une réglementation ;
- des manquements ou des situations contraires au code de conduite anticorruption SMI ;
- des risques d'atteinte graves liés aux activités du groupe Covéa dont SMI fait partie portant sur les droits humains, les libertés fondamentales, la santé et la sécurité des personnes, l'environnement.

Les types de données suivants sont traités :

- les données courantes d'identification (identité, fonction, direction de rattachement et coordonnées) que la personne soit l'émetteur du signalement (sous réserve de déclarer son identité, le signalement anonyme étant possible) ou qu'elle soit visée dans le signalement ;
- les éléments associés au signalement, dès lors qu'ils peuvent être rapprochés aux données (fait signalés et leurs éléments de vérification, compte-rendu des opérations de vérification, suites données au signalement).

3. Pourquoi les données sont-elles traitées ?

Les données sont utilisées afin de traiter les signalements de crime, délit, menace ou préjudice pour l'intérêt général, violation d'une réglementation, de manquements au code de conduite anticorruption ou de violations aux droits humains et libertés fondamentales, à la santé et à la sécurité des personnes et à l'environnement, et plus précisément :

- recueillir et traiter les signalements ;
- effectuer les vérifications, enquêtes et analyses nécessaires ;
- déterminer les suites à donner au signalement ;
- assurer la protection des personnes concernées, et notamment assurer une confidentialité de l'identité de l'auteur du signalement et des échanges ultérieurs avec celui-ci mais également des faits signalés et des personnes visées ;
- exercer ou défendre des droits en justice.

Cette finalité a pour base légale des obligations réglementaires de SMI.

De plus, une information relative à la protection des données personnelles est délivrée de façon spécifique à la personne visée dans le signalement, dans un délai raisonnable ne pouvant pas dépasser un mois à la suite de la réception du signalement, et par tout moyen adapté (courrier, e-mail). Toutefois, cette information peut être différée si elle est susceptible de compromettre gravement la réalisation des objectifs du traitement. Ainsi, cette information n'interviendra qu'après la prise de mesures conservatoires pour prévenir la destruction de preuves relatives aux faits signalés et après avoir établi la recevabilité du signalement.

4. À qui les données sont-elles destinées ?

Les données peuvent être communiquées, dans la limite de leurs missions et habilitations :

- aux personnes en charge du recueil et de la gestion des signalements au sein de SMI ;

- au(x) prestataire(s) au(x)quel(s) SMI est susceptible de sous-traiter la gestion de certaines activités ;
- aux experts missionnés pour les besoins de l'enquête ;
- à l'autorité judiciaire, le cas échéant.

5. Pendant combien de temps les données sont-elles conservées ?

La durée de conservation des données dépend du statut du signalement :

- les signalements reçus sont conservés jusqu'à la prise de décision définitive sur les suites à donner ;
- lorsqu'une décision définitive sur les suites à donner au signalement est prise :
 - soit le signalement n'est pas recevable car il n'entre pas dans le périmètre du dispositif d'alerte interne : les données sont conservées pendant une durée de trois mois à compter de la date où l'auteur du signalement est informé de la non-recevabilité de son signalement, afin de traiter les éventuelles interrogations de l'auteur du signalement vis-à-vis de cette décision ;
 - soit le signalement est recevable et aboutit à un classement sans suite ou donne lieu à des suites non disciplinaires ou non judiciaires : les données sont conservées pendant une durée d'un an à compter de la décision, afin de répondre aux finalités suivantes :
 - assurer la protection des différentes parties prenantes (auteur, facilitateur, personne mentionnée ou visée dans le signalement) contre le risque de représailles ;
 - permettre d'éventuelles enquêtes complémentaires ;
 - fournir des preuves sur le traitement du signalement en cas de contentieux ou de contrôles ultérieurs sur la conformité du processus de traitement des signalements (audit, autorité) ;
- soit le signalement est recevable et donne lieu à des suites disciplinaires ou judiciaires à l'encontre de la personne visée ou à l'encontre de l'auteur d'un signalement abusif : les données sont conservées jusqu'au terme de la procédure ou de la prescription des recours à l'encontre de la décision.

Au-delà de ces durées de conservation, les données sont anonymisées ou supprimées.

6. Où les données sont-elles traitées ?

Les données sont traitées en France. Exceptionnellement, les données peuvent être traitées en dehors de l'Union européenne sur la base d'une décision d'adéquation ou de conditions contractuelles négociées, qui sont disponibles auprès du délégué à la protection des données personnelles (DPO).

7. Quels sont les droits de la personne dont les données sont traitées ?

La personne dispose d'un droit d'accès, d'un droit de rectification, d'un droit d'effacement et d'un droit de limitation de ses données.

Le droit d'accès permet d'obtenir :

- la confirmation que des données la concernant sont (ou ne sont pas) traitées ;
- la communication d'une copie de l'ensemble des données personnelles détenues par le responsable de traitement la concernant.

La personne visée par un signalement ne pourra pas, sur le fondement de son droit d'accès, obtenir communication de l'identité de l'auteur du signalement ni des données relatives à des tiers.

Le droit de rectification permet de faire rectifier une information la concernant lorsque celle-ci est obsolète ou erronée. Il lui permet également de faire compléter des informations incomplètes la concernant.

Le droit d'effacement permet d'obtenir l'effacement des données personnelles sous réserve des durées légales de conservation. Il peut notamment trouver à s'appliquer dans le cas où les données ne seraient plus nécessaires au traitement.

Le droit de limitation permet de limiter le traitement des données dans les cas suivants :

- en cas d'usage illicite des données ;
- dans le cas où la personne conteste l'exactitude de celles-ci ;
- dans le cas où il est nécessaire pour la personne de disposer des données pour constater, exercer ou défendre ses droits.

La personne peut exercer ses droits aux adresses suivantes :

- pour les collaborateurs de SMI :
 - par courrier postal : Cellule protection des données – 2 rue de Laborde – CS 40041 -75374 Paris Cedex 08 ;
 - par email : protectiondesdonnees@mutuelle-smi.com.
- pour les autres personnes :
 - par courrier postal : Cellule protection des données – 2 rue de Laborde – CS 40041 -75374 Paris Cedex 08 ;
 - par email : protectiondesdonnees@mutuelle-smi.com.

La personne peut aussi définir des directives générales auprès d'un tiers de confiance ou particulières auprès du responsable du traitement concernant la conservation, l'effacement et la communication de ses données personnelles après son décès. Ces directives sont modifiables ou révocables à tout moment.

En cas de désaccord sur le traitement de ses données personnelles, la personne a la possibilité de saisir la Commission nationale de l'informatique et des libertés (CNIL).

8. Comment contacter le délégué à la protection des données ?

Pour toute information complémentaire, il est possible de contacter le délégué à la protection des données :

- pour les collaborateurs de SMI :
 - par courrier postal : Cellule protection des données – 2 rue de Laborde – CS 40041 -75374 Paris Cedex 08 ;
 - par email : protectiondesdonnees@mutuelle-smi.com.
- pour les autres personnes :
 - par courrier postal : Cellule protection des données – 2 rue de Laborde – CS 40041 -75374 Paris Cedex 08 ;
 - par email : protectiondesdonnees@mutuelle-smi.com.

Glossaire

Auteur de signalement

Il s'agit de la personne qui émet un signalement. L'auteur d'un signalement qui respecte toutes les conditions légales devient un lanceur d'alerte.

Autorités externes

En France, le dispositif d'alerte ne se substitue pas à la possibilité offerte par la loi au lanceur d'alerte de saisir directement ou à tout moment les autorités compétentes selon la loi applicable.

Il s'agit :

- de l'autorité judiciaire si les faits signalés constituent une infraction pénale (crime ou délit) ;
- des autorités compétentes en fonction du domaine concerné par le signalement.

Exemples

AUTORITÉ	COMPÉTENCE
ACPR (Autorité de contrôle prudentiel et de résolution)	Les services, produits et marchés financiers, la prévention du blanchiment des capitaux et le financement du terrorisme.
CNIL (Commission nationale de l'informatique et des libertés)	La protection de la vie privée et des données personnelles, la sécurité des réseaux et des systèmes d'information.
DGCCRF (Direction générale de la concurrence, de la consommation et de la répression des fraudes)	La protection des consommateurs et les pratiques anticoncurrentielles (marché intérieur).
DGT (Direction générale du travail)	Les relations individuelles et collectives du travail, des conditions de travail.

Défenseur des droits

Le Défenseur des droits est une autorité administrative indépendante qui veille au respect des droits et libertés des citoyens. Il est chargé d'accompagner les lanceurs d'alerte qui le sollicitent (information, conseil, aiguillage, soutien).

Il traite également les alertes dont il est saisi et qui relèvent de son domaine de compétence (discrimination, droits de l'enfant).

Divulgateur publique

Il s'agit du fait de rendre public son signalement, notamment au travers des médias.

Cette divulgation n'est possible qu'à certaines conditions prévues dans la loi pour pouvoir bénéficier du statut de lanceur d'alerte.

Facilitateur

C'est une personne qui aide le lanceur d'alerte :

- une personne physique : collègue, proche ;
- une personne morale de droit privé à but non lucratif : association, syndicat, ONG.

Le facilitateur qui a aidé le lanceur d'alerte dans le respect des règles légales peut bénéficier d'une protection identique à celle du lanceur d'alerte.

Lanceur d'alerte

C'est la personne qui a déclaré un signalement et qui répond à toutes les exigences de la loi pour pouvoir bénéficier du statut protecteur de lanceur d'alerte.

Mesures de représailles

Il s'agit de mesures négatives prises à l'encontre d'un lanceur d'alerte. Le Code du travail en liste 15 qui sont interdites si elles sont en lien avec le signalement.

Personne mise en cause

Il s'agit de la personne identifiée dans le signalement comme étant l'auteur des faits signalés.

Personne visée

Il s'agit de toute personne physique mentionnée dans le signalement :

- auteur présumé des faits signalés ;
- victime ;
- témoin.

Référent alertes

Personne désignée et habilitée pour recevoir et traiter les signalements entrant dans le champ du présent dispositif.

Signalement interne

Il s'agit d'un signalement réalisé auprès de l'entité concernée par les faits. Ce signalement implique de respecter la procédure interne de la structure professionnelle avec laquelle l'auteur du signalement est en lien pour bénéficier du statut de lanceur d'alerte.

Signalement externe

Il s'agit d'un signalement réalisé auprès des autorités externes compétentes.

Tiers autorisé

Tout tiers désigné par le Référent Alertes et/ou le comité d'éthique pour examiner tout ou partie des faits signalés.