Assurons
un monde
plus ouvert

CNP assurances

Procédure cadre de recueil et de traitement des alertes

A destination des Tiers

Direction de la Conformité Groupe (DCG)

Date de validité : janvier 2024

Émetteur	Direction de la Conformité Groupe
Version	V1
Statut	Validé
Périmètre d'application	Tous tiers avec une relation commerciale établie
Sujet	Procédure cadre de recueil et de traitement des alertes
Date d'application	Janvier 2024
Dernière date de mise à jour	Janvier 2024
Politiques et procédures liées	Code de conduite Groupe C@pEthic

Suivi des modifications

N° version	Détail des modifications
V1	Création de la procédure externe Groupe de recueil et de traitement des alertes

SOMMAIRE

1. INTRODUCTION 4

1.1 Objet de la présente procédure («la Procédure ») **4**

1.2 Périmètre et contexte **4**

2. Recours au lancement d'alerte 4

2.1 Eligibilité **4**

2.1.1 Domaines pouvant faire l'objet d'une alerte ou d'un signalement 4

2.1.2 Qualité de lanceur d'alerte 5

2.2 Lancement de l'alerte **6**

2.2.1 Modalités de lancement de l'alerte/du signalement 6

2.2.2 Contenu du signalement/alerte 6

2.2.3 Destinataires du signalement ou de l'alerte 6

3 Protection des personnes et les droits et devoirs de chacun des acteurs du dispositif d'alerte 7

3.1 Engagement des acteurs du dispositif d'alerte **7**

3.2 Protection du lanceur d'alerte **7**

3.2.1 Bénéficiaire de la protection 7

3.2.2 Confidentialité et anonymat 7

3.3 Protection des personnes faisant l'objet d'un signalement **8**

4 Traitement de l'alerte ou du signalement 9

4.1 Réception de l'alerte **9**

4.1.1 Accusé de réception 9

4.1.2 Classement du signalement 9

4.2 Traitement de l'alerte **10**

4.2.1 Devoir d'information tout au long du traitement 10

4.2.2 Investigations et instruction du dossier 10

4.2.3 Clôture de l'alerte 11

5. Les sanctions applicables en France 11

6. Traitement des données à caractère personnel 11

7. Durée de conservation des informations et archivage 12

7.1 Principe **12**

7.2 Exception **12**

ANNEXES 14

Annexe 1 « Liste des autorités externes instituées par la loi 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte » (applicable en France seulement) **14**

(Cf. Décret n° 2022-1284 du 3 octobre 2022 relatif aux procédures de recueil et de traitement des signalements émis par les lanceurs d'alerte) **14**

Annexe 2 « Liste des formes de représailles interdites » **17**

(Cf. article 10-1, II de la loi Sapin II modifiée) **17**

Annexe 3 « Mode opératoire de l'outil » **18**

1. INTRODUCTION

1.1 Objet de la présente procédure («la Procédure »)

La présente procédure d'alerte correspond, en outre, aux exigences légales notamment fixée par la loi n° 2016-1691 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, dite loi « Sapin II », modifiée par la loi 2021-041 du 24 mars 2022 dite loi « Waserman ».

Elle intègre également les exigences de la loi n° 2017-399 « Devoir de Vigilance » du 27 mars 2017 relative au devoir de vigilance des sociétés mères et entreprises donneuses d'ordre qui impose aux entités assujetties d'identifier et prévenir les risques d'atteintes graves envers les droits humains, les libertés fondamentales, la santé, la sécurité des personnes et la protection de l'environnement, résultant de leurs propres activités, celles de leurs filiales, de leurs sous-traitants et fournisseurs avec lesquels une relation commerciale est établie ainsi que celles fixées par le règlement européen sur la protection des données personnelles (« RGPD »)

La mise en place du dispositif d'alerte permet au Groupe de respecter la réglementation applicable en matière de lancement d'alerte par les Tiers[1] afin qu'ils puissent porter à la connaissance du Groupe tout manquement aux réglementations précitées et tout risque d'atteinte grave à la réputation des parties prenantes.

La présente Procédure est également fondée sur les documents de référence des actionnaires de CNP Assurances : La Banque Postale et la Caisse des Dépôts et Consignations. Elle présente le dispositif de recueil et de traitement des signalements/alertes susceptibles d'être reçus par les personnes habilitées au traitement des alertes (le « Dispositif »).

1.2 Périmètre et contexte

La présente Procédure s'applique à l'ensemble des Tiers tel que défini au paragraphe 2.1.2. Elle devra être mise à jour régulièrement, notamment en cas d'évolution législative ou réglementaire significative. Les évolutions entraînent, le cas échéant, la mise à jour des dispositifs de lancement d'alerte impactés.

L'absence ou la réalisation d'un signalement par un Tiers ne peut faire l'objet de sanctions ou de toute autre mesure de représailles ou de discrimination fondées sur ce motif.

Le présent Dispositif garantit la confidentialité des échanges, messages et pièces jointes échangés entre l'auteur du signalement/alerte et les personnes habilitées au traitement des alertes.

En tout état de cause, le Groupe veille à ce que tout lanceur d'alerte de bonne foi soit protégé comme indiqué ci-après.

2. Recours au lancement d'alerte

2.1 Eligibilité

L'alerte/signalement éthique est un dispositif contribue au respect des engagements éthiques et déontologiques du Groupe CNP Assurances et s'inscrit dans le dispositif global de lutte contre la corruption, défini par la Loi Sapin II et de la loi relative au devoir de vigilance.

Le dispositif d'alerte du Groupe traite à la fois de thématiques encadrées par la loi et de sujets ne revêtant d'aucune obligation légale ou réglementaire, mais qui sont susceptibles de porter un préjudice grave au Groupe dans la mesure où ils peuvent constituer une violation du Code de conduite Groupe « C@pEthic ».

Le recours au Dispositif est (i) ouvert à toute personne ayant la qualité de lanceur d'alerte au sens du § 2.1.2 de la présente Politique, (ii) sous réserve que le signalement et/ou l'alerte entrent dans le champ des domaines éligibles au lancement d'alerte au sens du § 2.1.1 de la présente Politique.

2.1.1 Domaines pouvant faire l'objet d'une alerte ou d'un signalement

Tout non-respect des règles et des valeurs du Groupe énoncées dans le Code de conduite Groupe « C@pEthic », dans la mesure où il pourrait être préjudiciable au Groupe ou porter atteinte aux droits humains, aux libertés fondamentales,

[1] *La notion de Tiers est définie au paragraphe 2.1.2*

à la santé et sécurité des personnes et à l'environnement[2]. Mais également, tout crime ou délit, toute violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, de la loi ou du règlement, ou toute menace ou préjudice graves pour l'intérêt général, est susceptible de faire l'objet d'une alerte ou d'un signalement de la part d'un Tiers.

Le Dispositif peut être utilisé notamment dans les domaines suivants :

- Domaines financier, comptable et bancaire ;
- Délinquance financière : corruption, trafic d'influence, blanchiment des capitaux et/ou financement du terrorisme, fraude interne ou externe, détournement de fonds … ;
- Pratiques anti-concurrentielles ;
- Santé et sécurité au travail, y compris la lutte contre les discriminations et le harcèlement au travail ;
- Protection de l'environnement
- Protection des données personnelles.

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.

La violation de ces secrets est passible de sanction pénale.

Par ailleurs, n'entre pas dans le champ d'application d'un signalement :

- Un simple dysfonctionnement interne à l'entreprise ;
- Un mécontentement lié à la relation avec le Groupe CNP Assurances ;
- Une infraction commise par un tiers n'agissant pas pour le compte du Groupe CNP Assurances ;
- Les réclamations commerciales usuelles doivent être adressées au service Réclamations compétent ;
- Les remontées d'alerte 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 de l'entité concernée.

2.1.2 Qualité de lanceur d'alerte

Tout Tiers qui a connaissance, dans le cadre de ses activités professionnelles ou non, de faits contraires à l'éthique, aux valeurs du Groupe ou aux lois et règlements et qui décide de faire un signalement aux personnes habilitées pour le recueil et le traitement des alertes, a la qualité de lanceur d'alerte.

Au sens de la présente Procédure, ont la qualité de « **TIERS** » :

- Les cocontractants de toute entité du Groupe liés par « une relation commerciale établie »[3], leurs sous-traitants et fournisseurs ou, lorsqu'il s'agit de personnes morales, les membres de l'organe d'administration, de direction ou de surveillance de ces cocontractants et sous-traitants ainsi que les membres de leur personnel.

NB : Il y a relation commerciale établie lorsque celle-ci revêt un caractère suivi, stable et habituel et où les parties peuvent raisonnablement anticiper pour l'avenir une certaine continuité du flux d'affaire avec son partenaire commercial. Les "relations commerciales" doivent en outre s'entendre au sens large, c'est-à-dire qu'elles s'appliquent à toutes relations commerciales, aussi bien à l'achat de produits que de services. Elles s'étendent au-delà des simples relations contractuelles et couvrent toutes formes de relations d'affaires, qu'elles fassent ou non l'objet d'un écrit.

---

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

[3] La notion de « relation commerciale établie » a été précisée dans un arrêt de la Cour de cassation, chambre commerciale, 20 mars 2012, n° 10-26.220

Pour avoir la qualité de lanceur d'alerte, le Tiers tel que défini ci-dessus doit agir de bonne foi et sans contrepartie financière directe ou indirecte.

En outre, lorsque les faits faisant l'objet d'une alerte ne sont pas produits dans le cadre de ses activités professionnelles, le lanceur d'alerte doit en avoir eu personnellement connaissance.

2.2 Lancement de l'alerte

2.2.1 Modalités de lancement de l'alerte/du signalement

L'usage recommandé est celui de la plateforme d'alerte en ligne CNP Integrity Line mise en place par le Groupe. Cette plateforme présente les meilleures garanties de sécurité et de confidentialité des échanges et informations relatives à l'alerte. Elle est accessible par tout Tiers du Groupe 24h/24h où qu'il se trouve, sans qu'il n'y ait besoin d'utiliser un ordinateur professionnel. Le formulaire est disponible dans les six langues utilisées dans le Groupe (anglais, français, espagnol, portugais, italien, grec). De plus, le texte d'alerte peut être rédigé dans n'importe quelle langue, la plateforme disposant d'un système de traduction.

Tout Tiers a également la possibilité d'adresser un signalement externe à une autorité compétente, au Défenseur des droits, à la justice ou à un organe européen, soit directement, soit après avoir effectué un signalement dans le cadre du Dispositif mis en place. Le décret en conseil d'état a dressé la liste des autorités externes instituées par la loi n° 2021-041 du 24 mars 2022 visant à améliorer la protection des lanceurs d'alerte (Annexe 1).

2.2.2 Contenu du signalement/alerte

Dans son signalement, l'auteur du signalement doit indiquer au minimum :

- Une description des faits.
- Quand les faits se sont produits ;
- Où les faits se sont produits (en indiquant, notamment, la société/filiale/succursale où les faits se sont produits) ;
- Quelle est sa préoccupation.

Le signalement peut être réalisé soit nominativement, soit de manière anonyme. Toutefois, pour faciliter le traitement du signalement, il est suggéré de donner le nom et prénom du Tiers, ainsi qu'une adresse électronique et un numéro de téléphone sur lequel il peut être joint. En tout état de cause, l'auteur du signalement bénéficie des garanties de confidentialité énoncées au § 3.2.2. de la présente Procédure.

La personne effectuant le signalement peut également, si elle le souhaite, indiquer/transmettre les éléments suivants :

- Nom, prénom, fonctions
- Société employeur ou lien avec le Groupe CNP Assurance
- Coordonnées
- Identité de la personne visée par le signalement (le cas échéant)
- Informations relatives à d'éventuels témoins
- Informations relatives à d'éventuels autres victimes
- Documents justificatifs

2.2.3 Destinataires du signalement ou de l'alerte

L'alerte effectuée via la plateforme web est reçue par les personnes habilitées au traitement des alertes. Seules ces dernières sont informées de l'existence d'un signalement dans l'outil.

3 Protection des personnes et les droits et devoirs de chacun des acteurs du dispositif d'alerte

3.1 Engagement des acteurs du dispositif d'alerte

Le Dispositif repose sur cinq piliers essentiels :

- La protection du lanceur d'alerte dès lors qu'il agit de bonne foi et de manière désintéressée ;
- La protection de tout tiers facilitateur (témoin, proche du lanceur d'alerte, etc.)
- La présomption d'innocence des personnes visées par l'alerte ;
- La bonne conduite des parties impliquées dans le recueil et le traitement de l'alerte ; et
- Le respect de la confidentialité.

Il garantit l'exercice impartial de sa mission et traite toute alerte reçue dans le cadre du dispositif de manière efficace, neutre et impartiale, dans le respect de la loi.

Pour traiter une alerte, les personnes habilitées au traitement des alertes peuvent s'adresser à des experts internes (ex : Juridique, protection des données, etc.) ou externes indépendants.

3.2 Protection du lanceur d'alerte

3.2.1 Bénéficiaire de la protection

Bénéficie de la protection octroyée au lanceur d'alerte :

- Toute personne éligible au sens du § 2.1.2 de la présente Procédure ;
- Tout facilitateur, c'est-à-dire toute personne physique ou morale de droit privé à but non lucratif qui aide un lanceur d'alerte à effectuer un signalement ou une divulgation ;
- Toute personne physique en lien avec un lanceur d'alerte, qui risque de faire l'objet de mesures de représailles dans le cadre de son activité professionnelle de la part de son employeur, de son client ou du destinataire de ses services ;
- Toutes entités juridiques contrôlées, au sens de l'article L. 233-3 du code de commerce, par un lanceur d'alerte, ou pour lesquelles il travaille, ou avec lesquelles il est en lien dans un contexte professionnel.

3.2.2 Confidentialité et anonymat

Le signalement peut être fait en toute confidentialité via l'outil Web qui garantit au lanceur d'alerte la confidentialité de la démarche. Le nom du lanceur d'alerte ne pourra être divulgué que dans le cas où la loi oblige cette divulgation. Le lanceur d'alerte doit également lui-même faire preuve d'une grande discrétion à l'égard de son signalement.

Lorsque la loi locale (lieu d'activité du Tiers) le permet, le signalement peut être anonyme. Dans ce cas, le lanceur d'alerte reçoit une référence de dossier pour pouvoir continuer la discussion avec le Groupe sans divulguer son nom.

Si, pour une raison quelconque, l'anonymat ne peut être garanti, le Groupe s'engage à garantir la confidentialité du signalement et à ne divulguer les éléments de nature à identifier le lanceur d'alerte qu'avec le consentement de celui-ci. Toutefois, le Groupe peut être amené à communiquer ces éléments à l'autorité judiciaire, dans le cas où il serait tenu de dénoncer les faits à celle-ci. Le lanceur d'alerte en serait alors informé, à moins que cette information ne risque de compromettre la procédure judiciaire.

Conformément à la loi Sapin II, tant le lanceur d'alerte que toute personne facilitant le lancement d'alerte ou encore l'entourage du lanceur d'alerte bénéficie de la protection prévue par la présente Procédure.

En application de la règlementation, le lanceur d'alerte de bonne foi ne peut pas faire l'objet de mesures de représailles, ni de menaces ou de tentatives de recourir à ces mesures, par suite du signalement.

Le lanceur d'alerte bénéficie des mesures de protection suivantes :

- Les lanceurs d'alerte, au sens de la loi, ne peuvent faire l'objet d'une mesure disciplinaire ou discriminatoire (directe ou indirecte) du fait de leur signalement (y compris les atteintes à la réputation via les réseaux sociaux (cf. annexe 2) ;
- Ils bénéficient d'une présomption de bonne foi dans le cadre de leur signalement et donc d'une inversion de la charge de la preuve ;
- Irresponsabilité pénale du lanceur d'alerte qui divulguerait des informations portant atteinte à un secret légal, y compris en cas de soustraction, détournement ou recel des documents confidentiels contenant des informations liées à son alerte à condition qu'il y ait eu accès de manière licite ;
- Peine d'amende de 30.000€ en cas d'action en diffamation contre un lanceur d'alerte ;
- Peine d'un an d'emprisonnement et de 15.000€ d'amende à l'encontre de toute personne faisant obstacle à la transmission d'un signalement ;
- Amende civile de 60.000€ en cas de procédure dilatoire ou abusive dirigée contre un lanceur d'alerte en raison des informations signalées ou divulguées ;
- Peine de trois ans de prison et de 45.000€ d'amende contre toute personne ayant discriminé un lanceur d'alerte ;
- Possibilité pour le juge d'allouer une provision pour frais de justice au lanceur d'alerte qui conteste une mesure de représailles.

3.3 Protection des personnes faisant l'objet d'un signalement

Il n'existe pas de protection légale de la personne faisant l'objet d'un signalement. Toutefois, toute personne visée par une alerte/signalement est présumée innocente jusqu'à ce que les allégations portées contre elle soient établies. Les personnes habilitées au traitement des alertes prennent toutes les précautions en vue de garantir la stricte confidentialité des éléments de nature à identifier les personnes visées par une alerte (identité, fonction, coordonnées).

Si le recours à des experts s'avère nécessaire dans le cadre de l'enquête, seules les informations strictement nécessaires sont communiquées et les personnes habilitées au traitement des alertes s'assurent que les personnes associées à l'enquête s'astreignent à une obligation de confidentialité renforcée s'agissant de l'identité de la personne visée.

La personne faisant l'objet d'un signalement peut être informée par les personnes habilitées au traitement des alertes, si les faits signalés relèvent d'un comportement purement individuel et si cette information permet de traiter le cas et d'y apporter une conclusion. Par exemple, si l'alerte signale des propos racistes, les personnes habilitées au traitement des alertes pourront s'adresser directement à la personne dont ils émanent.

Une personne faisant l'objet d'un signalement peut exercer son droit d'accès à l'information conformément au RGPD. Elle s'adressera alors au DPO (*Data Protection Officer* ou Délégué à la Protection des Données) du Groupe. Afin de garantir à toute personne visée par une alerte un droit d'accès et de rectification des données la concernant, les personnes habilitées au traitement des alertes doivent l'informer des faits qui lui sont reprochés. Lorsque des mesures conservatoires sont nécessaires, notamment pour prévenir la destruction de preuves relatives au traitement, l'information de cette personne intervient après l'adoption de ces mesures

Toutefois, la personne visée par un alerte ne peut en aucun cas obtenir sur le fondement de son droit d'accès, des informations concernant l'identité du lanceur d'alerte.

4 Traitement de l'alerte ou du signalement

4.1 Réception de l'alerte

Toute alerte ou tout signalement fait l'objet d'un traitement selon les étapes suivantes.

4.1.1 Accusé de réception

La personne qui reçoit l'alerte ou le signalement ou, à défaut, les personnes habilitées au traitement des alertes, accusent réception de l'alerte ou du signalement dans un délai de sept (7) jours à compter de la réception dudit signalement.

L'auteur de l'alerte ou du signalement peut transmettre, via la plateforme Integrity Line, tout élément, quel que soit sa forme et son support afin d'étayer les faits objet de son signalement.

4.1.2 Classement du signalement

Les personnes habilitées au traitement des alertes prennent connaissance du signalement et décident selon les critères définis ci-après de son classement, soit en classement sans suite, soit en classement recevable simple ou complexe.

4.1.2.1 Classement sans suite

Le signalement est classé sans suite lorsque :

- Il concerne un des domaines exclus par la loi (secret de la défense nationale, secret médical, secret des délibérations judiciaires, secret de l'enquête ou de l'instruction judiciaires et secret professionnel de l'avocat) ; ou
- Le sujet ne relève pas d'un des domaines prévus au § 2.1.2. En pareil cas, le lanceur d'alerte est informé, s'il a donné suffisamment d'informations pour pouvoir le contacter. Il peut être invité à adresser son signalement dans un autre cadre ; ou
- Il ne s'agit pas d'un signalement mais d'une simple question ;ou
- Une instruction simple détermine qu'il n'y a pas de sujet à traiter ; ou
- Les critères légaux (qualité du lanceur d'alerte et nature des faits) [4] ne sont pas respectés. Le cas échéant, le lanceur d'alerte est informé des raisons pour lesquelles il n'est pas donné de suite à son signalement.

L'auteur du signalement est informé du classement sans suite de son signalement. Les données sont effacées au plus tard deux mois après la décision de classement sans suite.

4.1.2.2 Signalement recevable

Lorsque le signalement ou l'alerte adressé est recevable, il fait d'abord l'objet, par les personnes habilitées au traitement des alertes, d'un classement selon les catégories suivantes :

- Blanchiment de capitaux et financement du terrorisme ;
- Pratiques commerciales déloyales ;
- Situation de conflits d'intérêts avérés ;
- Corruption/trafic d'influence ;
- Discrimination ;
- Fraude ;
- Santé ou sécurité au travail ;
- Harcèlement moral et sexuel ou agissements sexistes ;
- Détournement de fonds, malversations ;
- Non pertinent ; Autres Cas.

---

*[4] Par exemple, le lanceur d'alerte n'est pas une personne physique, il agit en contrepartie d'une rémunération financière directe, il est de mauvaise foi ou il n'a pas eu personnellement connaissance des informations qu'il a obtenues en dehors du cadre de ses activités professionnelles (cf. **article 6** pour les critères concernant la personne du lanceur d'alerte et **article 8, A, I** pour les critères concernant les faits, objet du signalement, de la loi Sapin II modifiée par la loi de mars 2022).*

Les personnes habilitées au traitement des alertes procèdent à une première analyse du signalement et décident de son classement en alerte simple ou en alerte complexe. Ce classement détermine qui accède à l'information et qui traite le signalement.

Alerte simple : Le signalement est classé dans cette catégorie lorsque l'analyse du dossier peut se faire par une personne chargée de la conformité, sur délégation et en l'absence de conflit d'intérêt, dans le pays où le signalement a été fait, et lorsque le traitement du dossier peut se faire rapidement. Ces signalements sont conservés pendant leur durée d'instruction et au maximum pendant un (1) an après clôture.

Alerte complexe : Le signalement est classé dans cette catégorie lorsque l'analyse du dossier nécessite une analyse plus approfondie et le recours à des experts ainsi qu'à des interlocuteurs spécifiques.

4.2 Traitement de l'alerte

4.2.1 Devoir d'information tout au long du traitement

Dans tous les cas, les personnes habilitées au traitement des alertes, prendront contact avec le Tiers ayant procédé au signalement, pour le tenir informé du résultat de l'analyse et ce, dans un délai maximum de trois (3) mois à compter de l'accusé de réception du signalement (ce délai de retour d'information de trois mois n'est pas applicable en cas d'alerte complexe nécessitant plus de temps et en cas de signalement anonyme.

A ce titre, le lanceur d'alerte sera averti par les personnes habilitées au traitement des alertes :

- Qu'ils entament les diligences nécessaires ;
- De l'avancement du traitement et des mesures envisagées dans un délai raisonnable n'excédant pas trois (3) mois à partir de l'accusé de réception ;
- De la désignation d'un expert, le cas échéant ;
- De la clôture du traitement.

4.2.2 Investigations et instruction du dossier

Le régime légal des lanceurs d'alerte nécessite de veiller à garantir la protection de leurs droits et notamment la stricte confidentialité de leur identité, mais également des faits objets du signalement et des personnes visées par le signalement.

Les personnes habilitées au traitement des alertes ont une stricte obligation de confidentialité :

- Ils s'interdisent de révéler le contenu de l'alerte, ou l'identité de son auteur aux personnes impliquées dans le signalement ;
- En cas de communication avec un expert, ils évaluent le volume et la pertinence des informations transmises et ne transmettent les informations qu'après avoir obtenu l'accord de l'auteur du signalement.

En cas de besoin, les personnes habilitées au traitement des alertes s'appuient sur une équipe (éventuellement locale) spécialement constituée à cet effet, pour répondre aux allégations contenues dans le signalement. Toute personne sollicitée dans le cadre de l'analyse à mener sera soumise aux mêmes obligations de confidentialité que les personnes habilitées au traitement des alertes. Le nombre d'experts sollicités doit être limité aux seules personnes dont les compétences sont nécessaires pour mener à bien les opérations d'instruction et d'investigation, afin de préserver la confidentialité du signalement. La communication des données personnelles et du contenu du signalement doit être en outre limitée aux seuls experts auxquels la connaissance de ces informations est indispensable pour mener à bien leur contribution au traitement du signalement. Le responsable de traitement veille à ne communiquer à l'expert que les informations qui lui sont nécessaires pour réaliser sa mission.

Le signalement/alerte fait obligatoirement l'objet d'un rapport, lequel est classé avec le signalement/alerte.

Le rapport d'analyse est porté immédiatement à la connaissance du Directeur Général lorsque la gravité des événements le justifie.

A la fin de l'instruction du dossier, le signalement/alerte fait l'objet, le cas échéant, d'une réponse au lanceur d'alerte dans un délai raisonnable n'excédant pas trois (3) mois à compter de l'accusé de réception, sous réserve d'avoir reçu l'intégralité des informations permettant l'instruction et sauf en cas d'alerte complexe nécessitant plus de temps.

Cette réponse présente les mesures envisagées ou prises pour évaluer l'exactitude des allégations et, le cas échéant, pour remédier à l'objet du signalement/alerte, ainsi que les motifs de ces mesures.

Enfin, après traitement, lorsque les allégations sont jugées inexactes ou infondées, ou lorsque le signalement/alerte est devenu sans objet, le signalement/alerte peut être clôturé.

4.2.3 Clôture de l'alerte

Les personnes habilitées au traitement des alertes clôturent l'alerte selon l'une des hypothèses suivantes :

- L'alerte est jugée fondée : traitement de la situation suivi d'un message de clôture à destination de l'auteur du signalement pour lui expliquer la manière dont a été traité son signalement, le cas échéant ;
- Les allégations sont inexactes ou infondées, ou lorsque le signalement est devenu sans objet : le signalement est clôturé et son auteur en est informé par écrit, le cas échéant ;
- Impossibilité de traitement du signalement : l'impossibilité de traitement est notifiée à l'auteur du signalement. Cette situation peut advenir lorsque l'auteur du signalement refuse toutes les propositions de traitement des personnes habilitées au traitement des alertes (transfert vers un service compétent, saisine d'experts…) etc.

5. Les sanctions applicables en France

Les textes régissant la protection des lanceurs d'alerte prévoient les sanctions suivantes :

- Concernant la confidentialité : Le fait de divulguer les éléments confidentiels est puni de deux ans d'emprisonnement et de 30 000 € d'amende.
- Concernant la protection contre les représailles : Si une procédure est dirigée contre un lanceur d'alerte en raison des informations signalées ou divulguées, le montant de l'amende est de 60 000 euros, sans préjudice de l'octroi de dommages et intérêts à la partie victime de la procédure dilatoire ou abusive.
- Concernant l'émission d'un signalement : Toute personne qui fait obstacle, de quelque façon que ce soit, à la transmission d'un signalement est punie d'un an d'emprisonnement et de 15 000 € d'amende.
- Par ailleurs, l'ensemble des dispositions de droit commun s'appliquent (notamment la responsabilité civile en cas de manquement à l'obligation de sécurité du salarié, la responsabilité pénale en cas de complicité d'atteinte à l'intégrité physique et mentale du salarié qui pourrait être retenu en cas de non-assistance à la suite d'une alerte, etc.).

6. Traitement des données à caractère personnel

Les signalements peuvent comporter des données à caractère personnel de leurs auteurs, des personnes qu'ils visent et des tiers qu'ils mentionnent. Ces données sont protégées et conservées pendant la durée nécessaire à leur traitement, en ce compris les délais d'éventuelles enquêtes complémentaires et/ou de procédures, et en conformité avec les obligations légales et réglementaires de conservation et de ces données. Des données relatives aux signalements peuvent toutefois être conservées au-delà de cette durée, à la condition que les personnes physiques concernées n'y soient ni identifiées, ni identifiables (anonymisation des données). Lorsqu'elles font l'objet d'un traitement, les données à caractère personnel relatives à des signalements sont conservées dans le respect du Règlement général européen sur la protection des données (RGPD).

Si des données sensibles au sens du RGPD ou des pièces jointes doivent être transférées pour le traitement du cas (par exemple à un expert indépendant), elles devront être anonymisées, sauf avis contraire du lanceur d'alerte. Si celui-ci refuse toute transmission alors que le traitement du cas l'exige, les personnes habilitées au traitement des alertes devront lui signifier qu'il n'est pas possible de traiter son signalement. Cette situation correspond à un cas extrême qui doit être évité dans la mesure du possible.

S'agissant des données d'infraction, leur collecte peut être autorisée :

- Par des dispositions spécifiques du droit national (par exemple, articles 8 et/ou 17 de la loi dite « loi Sapin II », article L 225- 102-4 du Code du commerce, etc.) ;
- Ou pour permettre au responsable de traitement « de préparer et, le cas échéant, d'exercer et de suivre une action en justice en tant que victime, mise en cause, ou pour le compte de ceux-ci », conformément à l'article 46-3° de la Loi Informatique et Liberté (LIL).

Les données considérées comme hors champ du dispositif sont supprimées directement. Il appartient aux personnes habilitées au traitement des alertes de rappeler à l'auteur d'un signalement que les informations communiquées dans le cadre d'un dispositif d'alerte doivent rester factuelles et présenter un lien direct avec l'objet de l'alerte.

Les Tiers qui sont concernés par l'alerte disposent d'un droit d'accès, de rectification, d'effacement, d'opposition et de limitation du traitement.

7. DUREE DE CONSERVATION DES INFORMATIONS ET ARCHIVAGE

7.1 Principe

Les signalements ne peuvent être conservés que le temps strictement nécessaire et proportionné à leur traitement à savoir pendant leur durée d'instruction et au maximum pendant un (1) an après clôture.

Si l'alerte n'est pas suivie d'une procédure disciplinaire ou judiciaire, **les données relatives à cette alerte** sont **supprimées** dans **un délai de deux mois après la clôture du cas**. Si une procédure disciplinaire ou contentieuse est engagée, les données relatives à ce cas peuvent être archivées dans l'outil CNP Integrity Line. Les cas archivés doivent être anonymisés (y compris les pièces jointes).

L'outil CNP Integrity Line adresse un message aux personnes habilitées au traitement des alertes après deux mois d'inactivité sur un cas. La suppression est automatique sans intervention humaine. Le cas peut alors demeurer actif ou être archivé en cas de procédure contentieuse par exemple. Le cas archivé doit être anonymisé.

Lorsque des données relatives à une alerte ont été échangées avec un expert, les personnes habilitées au traitement des alertes devront informer celui-ci de la clôture du cas et s'assurer qu'il supprime l'ensemble des données en sa possession.

7.2 Exception

A l'exception des cas où aucune suite n'est donnée à l'alerte, le responsable de traitement peut conserver certaines données collectées sous forme d'archives intermédiaires aux fins d'assurer la protection du lanceur de l'alerte ou de permettre la constatation des infractions continues. Les personnes habilitées au traitement des alertes en informent alors le lanceur d'alerte en lui indiquant qu'il reprendra contact avec lui pour s'assurer de sa situation.

Ces données doivent être sélectionnées et doivent exclusivement concourir à la protection du lanceur d'alerte au-delà de la clôture du cas. Un délai maximal de six mois après la clôture du cas pour recontacter le lanceur d'alerte et s'assurer qu'il n'a été victime d'aucunes représailles parait adapté. Si aucun problème n'apparait à l'issue de ce délai, les données seront supprimées. Dans le cas contraire, le lanceur d'alerte sera invité à adresser un nouveau signalement.

QUE FAUT-IL RETENIR ?

Le dispositif d'alerte

Il s'agit d'un dispositif qui contribue au respect des engagements éthiques et déontologiques du Groupe et qui s'inscrit dans le dispositif global de lutte contre la corruption, institué par la Loi Sapin II.

Ce dispositif permet également de remonter les alertes liées au devoir de vigilance (discriminations, harcèlement au travail, atteintes à la santé et à la sécurité au travail, et protection de l'environnement).

La plateforme d'alerte du Dispositif est facilement accessible pour les Tiers :

- soit sur le site institutionnel de CNP Assurances : https://www.cnp.fr/le-groupe-cnp-assurances/qui-sommes-nous/la-gouvernance/ethique-des-affaires
- soit en utilisant l'adresse URL : https://groupecnp.integrityline.app/.

La définition du lanceur d'alerte

Tout Tiers lié par une relation commerciale établie avec le Groupe qui a connaissance, dans le cadre de ses activités professionnelles ou non, de faits contraires à l'éthique, aux valeurs du Groupe ou aux lois et règlements et qui décide de faire un signalement aux personnes habilitées pour le recueil et le traitement des alertes.
Il agit de bonne foi et sans contrepartie financière. En outre, lorsque les faits faisant l'objet d'une alerte ne sont pas obtenus dans le cadre de ses activités professionnelles, il doit en avoir eu personnellement connaissance.

La protection du lanceur d'alerte

- La garantie de l'anonymat et la confidentialité des informations recueillies via le signalement/l'alerte
- Seules les personnes habilitées ont accès à l'alerte
- L'interdiction de mesures de représailles

Le traitement des signalements/alertes encadré par des délais

- Accusé de réception sous 7 jours
- Information du lanceur d'alerte sur le résultat de l'analyse dans un délai maximum de trois (3) mois - sous réserve de la réception de l'intégralité des informations permettant l'instruction et sauf en cas d'alerte complexe nécessitant plus de temps - (Δ non applicable en cas de signalement anonyme)
- Si classement sans suite, destruction des données sous 30 jours
- Si qualification d'alertes, conservation des données pour le temps strictement nécessaire et proportionné à leur traitement

CNP Integrity Line

- Un outil web sécurisé, conforme au RGPD
- Accessible par tout Tiers où qu'il se trouve
- Rédaction de l'alerte possible dans toutes les langues (la plateforme dispose d'un système de traduction automatique)

ANNEXES

Annexe 1 « Liste des autorités externes instituées par la loi 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte » (applicable en France seulement)

(Cf. Décret n° 2022-1284 du 3 octobre 2022 relatif aux procédures de recueil et de traitement des signalements émis par les lanceurs d'alerte)

1. Marchés publics :

- Agence française anticorruption (AFA), pour les atteintes à la probité ;

- Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF), pour les pratiques anticoncurrentielles ;

- Autorité de la concurrence, pour les pratiques anticoncurrentielles ;

2. Services, produits et marchés financiers et prévention du blanchiment de capitaux et du financement du terrorisme :

- Autorité des marchés financiers (AMF), pour les prestataires en services d'investissement et infrastructures de marchés ;

- Autorité de contrôle prudentiel et de résolution (ACPR), pour les établissements de crédit et organismes d'assurance ;

3. Sécurité et conformité des produits :

- Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) ;

- Service central des armes et explosifs (SCAE) ;

4. Sécurité des transports :

- Direction générale de l'aviation civile (DGAC), pour la sécurité des transports aériens ;

- Bureau d'enquêtes sur les accidents de transport terrestre (BEA-TT), pour la sécurité des transports terrestres (route et fer) ;

- Direction générale des affaires maritimes, de la pêche et de l'aquaculture (DGAMPA), pour la sécurité des transports maritimes ;

5. Protection de l'environnement :

- Inspection générale de l'environnement et du développement durable (IGEDD) ;

6. Radioprotection et sûreté nucléaire :

- Autorité de sûreté nucléaire (ASN) ;

7. Sécurité des aliments :

- Conseil général de l'alimentation, de l'agriculture et des espaces ruraux (CGAAER) ;

- Agence nationale chargée de la sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES) ;

8. Santé publique :

- Agence nationale chargée de la sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES) ;

- Agence nationale de santé publique (Santé publique France, SpF) ;

- Haute Autorité de santé (HAS) ;

- Agence de la biomédecine ;

- Etablissement français du sang (EFS) ;

- Comité d'indemnisation des victimes des essais nucléaires (CIVEN) ;

- Inspection générale des affaires sociales (IGAS) ;

- Institut national de la santé et de la recherche médicale (INSERM) ;

- Conseil national de l'ordre des médecins, pour l'exercice de la profession de médecin ;

- Conseil national de l'ordre des masseurs-kinésithérapeutes, pour l'exercice de la profession de masseur-kinésithérapeute ;

- Conseil national de l'ordre des sage-femmes, pour l'exercice de la profession de sage-femme ;

- Conseil national de l'ordre des pharmaciens, pour l'exercice de la profession de pharmacien ;

- Conseil national de l'ordre des infirmiers, pour l'exercice de la profession d'infirmier ;

- Conseil national de l'ordre des chirurgiens-dentistes, pour l'exercice de la profession de chirurgien-dentiste ;

- Conseil national de l'ordre des pédicures-podologues, pour l'exercice de la profession de pédicure-podologue ;

- Conseil national de l'ordre des vétérinaires, pour l'exercice de la profession de vétérinaire ;

9. Protection des consommateurs :

- Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) ;

10. Protection de la vie privée et des données personnelles, sécurité des réseaux et des systèmes d'information :

- Commission nationale de l'informatique et des libertés (CNIL) ;

- Agence nationale de la sécurité des systèmes d'information (ANSSI) ;

11. Violations portant atteinte aux intérêts financiers de l'Union européenne :

- Agence française anticorruption (AFA), pour les atteintes à la probité ;

- Direction générale des finances publiques (DGFIP), pour la fraude à la taxe sur la valeur ajoutée ;

- Direction générale des douanes et droits indirects (DGDDI), pour la fraude aux droits de douane, droits anti-dumping et assimilés ;

12. Violations relatives au marché intérieur :

- Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF), pour les pratiques anticoncurrentielles ;

- Autorité de la concurrence, pour les pratiques anticoncurrentielles et les aides d'Etat ;

- Direction générale des finances publiques (DGFIP), pour la fraude à l'impôt sur les sociétés ;

13. Activités conduites par le ministère de la défense :

- Contrôle général des armées (CGA) ;

- Collège des inspecteurs généraux des armées ;

14. Statistique publique :

- Autorité de la statistique publique (ASP) ;

15. Agriculture :

- Conseil général de l'alimentation, de l'agriculture et des espaces ruraux (CGAAER) ;

16. Education nationale et enseignement supérieur :

- Médiateur de l'éducation nationale et de l'enseignement supérieur ;

17. Relations individuelles et collectives du travail, conditions de travail :

- Direction générale du travail (DGT) ;

18. Emploi et formation professionnelle :

- Délégation générale à l'emploi et à la formation professionnelle (DGEFP) ;

19. Culture :

- Conseil national de l'ordre des architectes, pour l'exercice de la profession d'architecte ;

- Conseil des maisons de vente, pour les enchères publiques ;

20. Droits et libertés dans le cadre des relations avec les administrations de l'Etat, les collectivités territoriales, les établissements publics et les organismes investis d'une mission de service public :

- Défenseur des droits ;

21. Intérêt supérieur et droits de l'enfant :

- Défenseur des droits ;

22. Discriminations :

- Défenseur des droits ;

23. Déontologie des personnes exerçant des activités de sécurité :

- Défenseur des droits.

Annexe 2 « Liste des formes de représailles interdites »

(Cf. article 10-1, II de la loi Sapin II modifiée)

En application de la règlementation applicable au Groupe, le lanceur d'alerte de bonne foi ne peut faire l'objet d'aucune mesure de représailles, ni de menace ou de tentative de recourir à ces mesures, par suite du signalement, notamment sous les formes suivantes :

1° Suspension, mise à pied, licenciement ou mesures équivalentes ;

2° Rétrogradation ou refus de promotion ;

3° Transfert de fonctions, changement de lieu de travail, réduction de salaire, modification des horaires de travail ;

4° Suspension de la formation ;

5° Evaluation de performance ou attestation de travail négative ;

6° Mesures disciplinaires imposées ou administrées, réprimande ou autre sanction, y compris une sanction financière ;

7° Coercition, intimidation, harcèlement ou ostracisme ;

8° Discrimination, traitement désavantageux ou injuste ;

9° Non-conversion d'un contrat de travail à durée déterminée ou d'un contrat temporaire en un contrat permanent, lorsque le travailleur pouvait légitimement espérer se voir offrir un emploi permanent ;

10° Non-renouvellement ou résiliation anticipée d'un contrat de travail à durée déterminée ou d'un contrat temporaire ;

11° Préjudice, y compris les atteintes à la réputation de la personne, en particulier sur un service de communication au public en ligne, ou pertes financières, y compris la perte d'activité et la perte de revenu ;

12° Mise sur liste noire sur la base d'un accord formel ou informel à l'échelle sectorielle ou de la branche d'activité, pouvant impliquer que la personne ne trouvera pas d'emploi à l'avenir dans le secteur ou la branche d'activité ;

13° Résiliation anticipée ou annulation d'un contrat pour des biens ou des services ;

14° Annulation d'une licence ou d'un permis ;

15° Orientation abusive vers un traitement psychiatrique ou médical.

Annexe 3 « Mode opératoire de l'outil »

1. Accès à l'outil

Le Tiers peut accéder au dispositif d'alerte Groupe au moyen d'un lien directement accessible en bas de la page « Ethique des affaires » du site institutionnel de CNP Assurances « Lancer une alerte éthique » ou directement via le lien : https://groupecnp.integrityline.app/.

Le dispositif est également accessible par le biais du QR Code suivant :

2. Rédaction d'un signalement/alerte

1- Cliquez sur « Soumettre une alerte », un formulaire de saisie s'ouvre automatiquement, présentant des zones à renseigner.

2- Une boite postale sécurisée est créée automatiquement après saisie du mot de passe suivi d'un simple clic « envoyer »

3. Confirmation de réception

Un écran final confirme l'enregistrement de l'alerte sans reprendre les termes du signalement/alerte.

Il y est indiqué les modalités de suivi pour le Tiers :

- Le mot de passe et la référence de dossier affecté à son signalement/alerte.
- Le mot de passe est à conserver impérativement par le lanceur d'alerte. Pour des raisons de confidentialité, l'outil ne peut pas réinitialiser le mot de passe en cas de perte ou d'oubli ;
- Le Tiers se connecte en cliquant sur l'onglet « Boite postale sécurisée » avec son mot de passe et la référence du dossier. Le retour d'information des personnes habilitées au traitement des alertes est accessible depuis sa boite postale sécurisée.

La référence du dossier peut être retrouvée depuis l'onglet « détails » de la boite postale sécurisée.