Procédure d’alerte interne

Version juillet 2025

SOMMAIRE

CHAMP D'APPLICATION 3
QUI PEUT ETRE LANCEUR D'ALERTE ? 3
SUR QUOI PEUT PORTER L'ALERTE ? 4
QUELLE CONFIDENTIALITE ? 5
AUPRES DE QUI LANCER L'ALERTE ? 6
Le choix de la procédure de signalement : interne ou externe 6
Le signalement interne 6
Le signalement externe 6
Divulgation publique 7
RECUEIL DES SIGNALEMENTS INTERNES 7
Auprès de qui lancer l'alerte 7
Le contenu de l'alerte 7
Le traitement de l'alerte 8
Réception de l'alerte 8
Analyse de l'alerte 8
Procédure d'enquête en vue du traitement de l'alerte 8
Résolution – Suite à donner à l'alerte 9
LE SIGNALEMENT EXTERNE : SAISINE d'UNE AUTORITE DESIGNEES PAR LA LOI 9
LA POLITIQUE DE TRAITEMENT DES DONNEES 10
Quelles sont les données traitées ? 10
Durée de conservation 10
Destruction des données, mesures de sécurité 11
Données à caractère personnel 11
SUIVI DES ALERTES 12
LA PUBLICITÉ SUR LE DISPOSITIF D'ALERTE INTERNE 12
A RETENIR 12

CHAMP D'APPLICATION

La Procédure d'alerte constitue l'un des piliers du Dispositif Ethique & Conformité du Groupe GINGER.

Cette Procédure d'alerte permet à l'ensemble des collaborateurs du groupe GINGER et à ses parties prenantes :

- de signaler, en toute confidentialité, sans crainte de pressions ou de représailles, des informations portant sur un crime, un délit, une menace ou un préjudice pour l'intérêt général ;
- des manquements ou des situations contraires à notre code de conduite anticorruption ou à notre charte éthique ;
- de s'informer de l'état d'avancement du traitement d'un signalement déjà réalisé.

Le dispositif légal français encadrant cette procédure est le suivant :

- la loi dite « Sapin II »[1] au titre des dispositions sur la protection des lanceurs d'alerte (art. 6-16) et des dispositions sur les mesures de lutte contre la corruption (art. 17) ;
- la directive européenne sur la protection des lanceurs d'alerte[2] ;
- les lois françaises relatives à la protection des lanceurs d'alerte et au recueil et traitement des signalements émis par les lanceurs d'alerte[3] ; et
- les réglementations de droit commun en matière de protection des personnes (notamment les dispositions concernant les discriminations de toutes natures, le harcèlement moral, le harcèlement sexuel…).

Lorsque que, dans un autre pays que la France, la réglementation locale relative au lanceur d'alerte est plus protectrice et/ou exigeante, il convient d'appliquer la législation locale et non la présente Procédure. A l'inverse, si la présente Procédure prévoit des règles plus protectrices et/ou exigeantes, c'est cette Procédure qui prévaut.

QUI PEUT ETRE LANCEUR D'ALERTE ?

Le lanceur d'alerte peut être toute partie prenante interne ou externe. Autrement dit, il peut s'agir :

- **des collaborateurs** du Groupe GINGER (salariés en contrat à durée indéterminée, salariés en contrat à durée déterminée, stagiaires, apprentis et également les intérimaires) ;
- **des mandataires sociaux** du Groupe ;
- **des tiers parties prenantes** étant en relation avec le Groupe GINGER ou ayant des intérêts avec le Groupe GINGER (clients, fournisseurs, co-traitants, sous-traitants, experts extérieurs, intermédiaires, actionnaires, Etat, associations, syndicats…).

[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, et son décret d'application n°2017-564 du 19 avril 2017. Cette Politique a valeur de 'procédure interne' au sens du décret.

[2] Directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union Européenne.

[3] Loi organique n°2022-400 et loi ordinaire n°2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte et Décret n°2022-1284 du 3 octobre 2022 relatif aux procédures de recueil et de traitement des signalements émis par les lanceurs d'alerte

Au surplus, pour pouvoir être qualifié de lanceur d'alerte, la loi prévoit les conditions cumulatives de recevabilité suivantes :

- le lanceur d'alerte doit être une **personne physique** ;
- le lanceur d'alerte doit agir **sans contrepartie financière directe** ;
- le lanceur d'alerte doit agir de **bonne foi** (sans intention de nuire).

Lorsque les informations ont été obtenues :

- le lanceur d'alerte qui n'a pas d'interaction avec le groupe doit avoir eu personnellement connaissance des informations qu'il signale ;
- le lanceur d'alerte qui a des interactions avec le groupe (salarié, fournisseur…) pourra signaler des informations dont il a eu personnellement connaissance mais également des informations qui lui ont été rapportées.

Le lanceur d'alerte peut choisir de rester anonyme, ce qui, d'un point de vue pratique, peut rendre plus difficile voire impossible le traitement du signalement ou l'établissement de la véracité des faits.

SUR QUOI PEUT PORTER L'ALERTE ?

Sous réserve des conditions de recevabilité, un signalement susceptible de constituer une alerte consiste à révéler de bonne foi notamment :

- un crime ou un délit :
    - à titre d'exemple : des faits de corruption, des faits de trafic d'influence, des faits de blanchiment d'argent ;
- une violation ou une tentative de dissimulation d'une violation :
    - de la loi ou du règlement
        - à titre d'exemple :
            - non-respect des réglementations de lutte contre le travail dissimulé, le travail forcé, le travail des enfants ;
            - des faits de harcèlement moral ou de harcèlement sexuel ;
            - non-respect de la réglementation santé et sécurité au travail
            - non-respect du droit de l'environnement ;
    - du droit de l'Union européenne ;
    - 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 ;
- une menace ou un préjudice grave pour l'intérêt général;
- une violation de la charte éthique du Groupe GINGER ;
- une violation du code de conduite anticorruption du Groupe GINGER ;
- une violation des procédures Groupe ;
- des actes de représailles liés au fait d'avoir fait un signalement ou participé à son traitement ;
- une divulgation d'information confidentielle ;
- un vol de data, appropriation frauduleuse d'actifs ;
- une fraude sur les déclarations financières ;
- une violation de droits humain.

Le lanceur d'alerte ne peut pas révéler d'informations couvertes par le secret de la Défense Nationale, le secret médical ou le secret des relations entre un avocat et son client.

Seules les informations présentant un caractère illicite ou portant atteinte à l'intérêt général peuvent faire l'objet d'un signalement ou d'une divulgation. De simples dysfonctionnements dans une entité publique ou privée ne peuvent fonder une alerte.

Seule une personne répondant aux critères ci-dessus peut être qualifiée de lanceur d'alerte et bénéficier ainsi du régime de protection des lanceurs d'alerte prévu par la loi. Cette protection lui garantit son anonymat.

Le lanceur d'alerte qui agit de bonne foi sans contrepartie financière directe ne peut être écarté d'une procédure de recrutement, de l'accès à un stage ou à une formation professionnelle.

Lorsque le lanceur d'alerte est un salarié, il ne peut être sanctionné, licencié ou faire l'objet d'une mesure discriminatoire, pour avoir signalé une alerte. Ainsi, toute mesure de représailles, directe ou indirecte, à l'encontre d'un collaborateur qui a signalé une alerte, ne saurait être tolérée.

En cas de sanction ou de licenciement lié à l'exercice du droit d'alerte, le lanceur d'alerte a la possibilité de saisir en référé le conseil des prud'hommes.

La protection du lanceur d'alerte n'a vocation à s'appliquer que lorsque ce dernier a agi de bonne foi et de manière désintéressée, comme indiqué ci-avant, sans chercher à nuire au Groupe.

L'utilisation abusive autrement dit l'utilisation 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 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.

L'utilisation abusive du dispositif d'alerte peut exposer son auteur à des sanctions diverses, dont en particulier :

- une procédure disciplinaire pouvant aller jusqu'au licenciement pour faute selon la gravité des faits reprochés ;
- des poursuites pénales pour délit de dénonciation calomnieuse (puni de 5 ans d'emprisonnement et de 45 000 € d'amende en France), abus de confiance (puni de 3 ans d'emprisonnement et 375 000 € d'amende), et/ou suppression ou altération de données informatiques (puni de 3 ans d'emprisonnement et 100 000 € d'amende), etc. ;
- engagement de sa responsabilité civile vis-à-vis de la victime de la dénonciation calomnieuse.

QUELLE CONFIDENTIALITE ?

La Procédure d'alerte interne permet de garantir la confidentialité de l'identité de l'auteur de l'alerte, l'identité de la personne visée et des informations recueillies.

Les éléments de nature à identifier l'auteur de l'alerte ne peuvent être divulgués qu'à l'autorité judiciaire à condition que l'auteur de l'alerte ait donné son consentement.

Dès lors que le caractère fondé de l'alerte est établi, les éléments de nature à identifier la personne visée par l'alerte pourront être uniquement divulgués à l'autorité judiciaire.

Toute autre divulgation est interdite.

Toute personne qui aurait connaissance, dans le cadre de la procédure d'alerte, de ces informations est soumise à une obligation de confidentialité.

AUPRES DE QUI LANCER L'ALERTE ?

Le choix de la procédure de signalement : interne ou externe

La loi prévoit deux manières de lancer une alerte : en procédant à un **signalement interne** ou à un **signalement externe**.

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.

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

Pour bénéficier du régime de protection du lanceur d'alerte, la divulgation publique (par exemple auprès des médias) ne peut être envisagée qu'après un signalement externe.

Le signalement interne

La possibilité d'effectuer un signalement interne appartient aux personnes en interaction avec la société concernée (salariés, mandataires sociaux, tiers parties prenantes).

Ainsi les personnes physiques qui ont obtenu, dans le cadre de leurs activités professionnelles, des informations portant sur des faits qui se sont produits ou sont très susceptibles de se produire dans l'entreprise concernée, peuvent signaler ces informations par la voie interne, notamment lorsqu'elles estiment qu'il est possible de remédier efficacement à la violation par cette voie et qu'elles ne s'exposent pas à un risque de représailles.

Le signalement externe

Il est possible d'adresser un signalement externe, soit après avoir effectué un signalement interne, soit directement au choix auprès :

- **de l'une des autorités compétentes** désignées en annexe du décret n°2022-1284 du 3 octobre 2022 , choisie en fonction du domaine concerné par l'alerte (Annexe 1 de la présente procédure)

  Par exemple, pour les signalements portant sur les relations individuelles et collectives du travail et/ou les conditions de travail, l'autorité désignée est la Direction générale du travail (DGT). En matière d'emploi et de formation professionnelle, il s'agit de la Délégation générale à l'emploi et à la formation professionnelle (DGEFP) et, pour ce qui touche aux discriminations, au Défenseur des droits.

  Autres exemples : pour une alerte concernant les activités du ministère de la Défense, le contrôle général des armées ; pour une alerte portant sur des faits de corruption, l'Agence Française Anticorruption.

- **du Défenseur des droits** qui selon les cas :

- *Oriente le lanceur d'alerte vers les autorités compétentes pour traiter le signalement ;*
- *Traite le signalement dans ses propres domaines de compétence : droits de l'enfant, discriminations, déontologie des personnes exerçant des activités de sécurité et relations avec les services publics.*

- **de l'autorité judiciaire :**
  Par exemple : au Procureur de la République si le lanceur d'alerte pense signaler un crime ou délit.

- **d'une institution, d'un organe ou d'un organisme de l'Union européenne compétent** pour recueillir des informations sur des violations relevant du champ d'application de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019
  Par exemple : saisine de L'Office européen de lutte antifraude sur une fraude concernant le budget de l'Union.

Divulgation 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.

RECUEIL DES SIGNALEMENTS INTERNES

Auprès de qui lancer l'alerte

Le lanceur d'alerte adresse son signalement au Référent éthique joignable à l'adresse email suivante :

referent.ethique@groupeginger.com

Cette adresse mail n'est consultable que par le Référent éthique du Groupe Ginger.

Le Référent éthique est le directeur/la directrice des ressources humaines Groupe.

Le contenu de l'alerte

Afin de pouvoir être traitée, toute alerte doit :

- être rédigée en langue française ou anglaise ;
- concernant l'identité, le lanceur d'alerte a 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 impossible d'assurer sa 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.
- indiquer l'identité et les fonctions de la personne faisant objet du signalement ;
- énoncer les faits signalés ;
- fournir toutes informations ou documents de nature à étayer son signalement et la gravité des faits signalés.

Ces éléments permettront ensuite au Référent éthique d'analyser et d'enquêter sur les faits révélés.

Le traitement de l'alerte

Réception de l'alerte

A la réception de l'alerte via l'adresse mail dédiée, le Référent éthique :

- envoie d'un accusé de réception du signalement, dans un délai de sept jours ;
- indique au lanceur d'alerte les modalités suivant lesquelles il sera informé des suites données à son signalement ;

Le Référent éthique peut décider de ne pas informer à réception de l'alerte la personne visée par le signalement, s'il dispose d'éléments fiables et matériellement vérifiables, afin de prévenir la destruction de preuves relatives à l'alerte.

Toute personne faisant l'objet d'un signalement dans le cadre de l'alerte interne est présumée innocente jusqu'à ce que les allégations portées contre elle soient établies.

A compter de la réception de l'alerte, le Référent éthique dispose d'un délai d'un mois pour confirmer au lanceur d'alerte la prise en compte de son alerte et pour commencer la procédure d'enquête.

A compter de la réception de l'alerte, le Référent éthique dispose d'un délai maximum de trois mois pour traiter ladite alerte.

Le Référent éthique prend toutes les mesures nécessaires afin de protéger l'identité du déclarant signalant une alerte ainsi que des personnes visées par l'alerte et la nature des faits.

Il ne peut en référer qu'au représentant légal de la société où a lieu l'alerte.

Les alertes sont traitées en toute confidentialité, ainsi que les enquêtes et rapports subséquents, sous réserve des obligations découlant de la loi ou des procédures judiciaires applicables.

Analyse de l'alerte

A réception du signalement, le Référent :

- analyse le caractère sérieux des faits allégués et la recevabilité de l'alerte ;
- procède le cas échéant à des vérifications complémentaires ;
- après examen du caractère sérieux des faits invoqués et de la précision des informations données, le Référent décide du traitement de cette alerte, met en œuvre une enquête et qualifie les faits.

Procédure d'enquête en vue du traitement de l'alerte

Le Référent éthique liste les actions à mener et organise une enquête interne (recherche de preuves, recherches informatiques, auditions de personnes, etc.) afin de déterminer la réalité et la matérialité des faits signalés.

Le cas échéant, des échanges préservant la confidentialité de l'identité du lanceur d'alerte pourront être organisés avec ce dernier.

Le Référent éthique établira un rapport d'enquête.

Résolution – Suite à donner à l'alerte

A l'issue de l'examen de l'alerte par le Référent éthique, le lanceur d'alerte est informé dans les 3 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,
- le cas échéant, les mesures de remédiation mises en œuvre.

LE SIGNALEMENT EXTERNE : SAISINE d'UNE AUTORITE DESIGNEES PAR LA LOI

Le lanceur d'alerte peut saisir une autorité externe. Il n'est pas nécessaire d'avoir au préalable procédé à une alerte interne.

La loi a fixé une liste d'autorités pouvant être saisies par les lanceurs d'alerte, désignées sous le nom d'autorités externes. La liste des autorités externes figure en annexe de la présente procédure.

Les autorités externes sont tenues de mettre disposition, sur leur site internet, les règles de procédure qu'elles appliquent ainsi que les moyens qui permettent de les saisir.

La procédure peut être un peu différente pour chaque autorité mais elle doit permettre au minimum de savoir :

- le champ de compétence de l'autorité ;
- à qui adresser le signalement (coordonnées postales, téléphoniques, électroniques) ;
- quelles informations transmettre ;
- quelles précautions doivent être prises pour préserver la confidentialité de l'alerte ;
- comment l'alerte va être traitée (voie postale, messagerie, etc.) ;
- les coordonnées du Défenseur des droits.

La procédure prévue au sein de l'autorité doit notamment comporter les garanties suivantes :

- la possibilité d'adresser un signalement par écrit et par oral ;
- l'envoi d'un accusé de réception du signalement, dans un délai de sept jours ;
- la garantie de l'intégrité et de la confidentialité des données recueillies (identité du lanceur d'alerte et de la personne mise en cause) ;
- le traitement du signalement par un personnel doté d'une autorité et de moyens suffisants ;
- la communication par écrit des informations sur les mesures envisagées ou prises pour évaluer l'exactitude de vos allégations et, le cas échéant, remédier à l'objet du signalement ;
- les délais de réponse

Les délais de réponse varient selon l'autorité saisie et la nature du dossier.

LA POLITIQUE DE TRAITEMENT DES DONNEES

Quelles sont les données traitées ?

Seules les données nécessaires à la vérification des faits peuvent être traitées.

Il s'agit de :

- le cas échéant, l'identité, les fonctions et les coordonnées de l'émetteur de l'alerte ;
- l'identité, les fonctions et les coordonnées des personnes faisant l'objet de l'alerte ;
- l'identité, fonctions et coordonnées des personnes intervenant dans le recueil ou dans le traitement de l'alerte ;
- les faits signalés ;
- les éléments recueillis dans le cadre de la vérification des faits signalés ;
- le compte rendu des opérations de vérification ;
- les suites données à l'alerte.

La personne qui fait l'objet d'un signalement dans le cadre d'une alerte interne ne peut en aucun cas obtenir, sur le fondement de son droit d'accès, des informations concernant l'identité de l'auteur de l'alerte.

La confidentialité pourra être levée dans les cas suivants :

- divulgation de l'identité du lanceur d'alerte avec son consentement ;
- divulgation de la personne mise en cause par l'alerte une fois le caractère fondé de l'alerte établi ;
- transmission à l'autorité judiciaire.

Durée de conservation

La durée de conservation des données dépend du statut de l'alerte :

- Les alertes reçues sont conservées jusqu'à la prise de décision définitive sur les suites à donner.
- Lorsqu'une décision définitive sur les suites à donner à l'alerte est prise :
    - Soit l'alerte 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 de l'alerte est informé de la non-recevabilité de son alerte, afin de traiter les éventuelles interrogations de l'auteur de l'alerte vis-à-vis de cette décision.
    - Soit l'alerte est recevable et aboutit à un classement sans suite ou donne lieu à des suites non disciplinaires ou non judicaires : 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 l'alerte) 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 alerte (audit, autorité).

- Soit l'alerte 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'une alerte abusive : 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.

Destruction des données, mesures de sécurité

Le Référent éthique prend toutes mesures utiles pour préserver la sécurité et la confidentialité des données, tant à l'occasion de leur recueil, de leur traitement, de leur conservation que de leur communication (ex : accès restreint sur un serveur sécurisé, coffre, etc.)

Si l'alerte entre dans le champ d'application du dispositif d'alerte, alors le Référent procède à la destruction de toutes les données communiquées dans les délais suivants :

- Les données à caractère personnel recueillies qui ne sont pas suivies d'une procédure disciplinaire ou judiciaire sont détruites ou archivées, après anonymisation, dans un délai de deux mois à compter de la fin d'analyse de la recevabilité ou de clôture des opérations de vérification ;
- Lorsqu'une procédure disciplinaire ou des poursuites judiciaires sont engagées à l'encontre de la personne mise en cause ou de l'auteur d'une alerte abusive, les données relatives à l'alerte sont détruites par le Référent éthique après la clôture de la procédure disciplinaire ou judiciaire engagée.

Données à caractère personnel

Toute donnée à caractère personnel communiquée par un lanceur d'alerte en application du présent dispositif d'alerte sera traitée conformément aux dispositions légales applicables en matière de protection et traitement des données à caractère personnel.

Ces données sont collectées dans le but de se conformer à la loi Sapin II, et plus généralement aux obligations légales applicables au Groupe GINGER. Elles seront enregistrées dans un fichier informatisé, pourront être transmises aux autorités administratives et judiciaires compétentes.

La durée de conservation de ces données est limitée à la durée mentionnée dans la présente Procédure.

L'émetteur de l'alerte ou la personne faisant l'objet d'une alerte peuvent accéder aux données les concernant et en demander, si elles sont inexactes, incomplètes, équivoques ou périmées, leur rectification ou leur suppression.

La demande est à formuler auprès du Référent éthique, responsable du traitement de l'alerte en utilisant l'adresse e-mail dédiée.

L'émetteur de l'alerte ou la personne faisant l'objet d'une alerte peuvent se faire assister par toute personne de leur choix appartenant à l'entreprise et ce, à tous les stades du dispositif.

SUIVI DES ALERTES

Afin de pouvoir évaluer l'efficacité du dispositif d'alerte, la personne en charge du traitement de l'alerte met en place un suivi annuel statistique concernant la réception, le traitement et les suites des alertes.

Ce suivi annuel statistique fait apparaître le nombre d'alertes reçues, de dossiers clos, de dossiers ayant donné ou donnant lieu à une enquête, le nombre et le type de mesures prises pendant et à l'issue de l'enquête (mesures conservatoires, engagement d'une procédure disciplinaire ou judiciaire, sanctions prononcées, etc.).

LA PUBLICITÉ SUR LE DISPOSITIF D'ALERTE INTERNE

La connaissance du dispositif d'alerte par les collaborateurs et les parties prenantes externes est indispensable à son efficacité. L'ensemble du personnel de GINGER 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.

Les tiers sont informés de l'existence du dispositif grâce à des informations sur le site institutionnel www.groupeginger.com

A RETENIR

☒ Le présent dispositif d'alerte est instauré en application de la Loi Sapin II.

☒ Il ne constitue pas une obligation mais une option supplémentaire offerte aux collaborateurs et aux parties prenante.

☒ Le dispositif définit les modalités de lancement et de traitement d'une alerte par un collaborateur ou une partie prenante.

☒ Le lanceur d'alerte n'encourt aucune sanction en cas d'alerte de bonne foi, comme décrit au présent dispositif. Sauf exception, son identité restera confidentielle tout au long du traitement de l'alerte.

☒ Une utilisation abusive du dispositif d'alerte peut exposer son auteur à des sanctions.

*****

ANNEXE

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 sages-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.