



RH & CONFORMITÉ

PROCÉDURE D'ALERTE INTERNE

Page 1 sur 25

Révision : v1.0

Date : 10/07/2023

PROCÉDURE D'ALERTE INTERNE

USAGE EXTERNE

Exail Proprietary

SOMMAIRE

I.	GLOSSAIRE.....	3
II.	CADRE DU DISPOSITIF D'ALERTE INTERNE	4
III.	CHAMP D'APPLICATION DU DISPOSITIF.....	5
IV.	RÉFÉRENTS ET COMITÉS.....	8
V.	COMMENT LANCER UNE ALERTE	11
VI.	COMMENT EST RECEPTIONNÉE UNE ALERTE.....	14
VII.	COMMENT EST TRAITÉE UNE ALERTE.....	15
VIII.	CONFIDENTIALITÉ.....	17
IX.	PROTECTION DU LANCEUR D'ALERTE.....	18
X.	DROITS DES PERSONNES VISÉES PAR UNE ALERTE.....	19
XI.	TRAITEMENT DES DONNÉES PERSONNELLES.....	20
XII.	CONSERVATION ET DESTRUCTION DES DONNÉES.....	21
XIII.	SANCTIONS.....	22
XIV.	INFORMATION ET SENSIBILISATION.....	23
XV.	A RETENIR	24
XVI.	ANNEXES	25

I. GLOSSAIRE

AFA : Agence Française Anticorruption

CGA/CGV : Conditions Générales d'Achat / Conditions Générales de Vente

CNIL : Commission Nationale de l'Informatique et des Libertés

Code : désigne le *Code de conduite anticorruption* du groupe Exail.

Collaborateur : désigne collectivement pour chaque Entité : (i) les employés, qu'ils travaillent à temps plein, à temps partiel, en CDD, en CDI, sous convention de thèse, en situation d'alternance ou d'apprentissage ; (ii) les personnels en situation de portage salarial, (iii) les intérimaires et stagiaires ; (iv) les dirigeants non-salariés et personnes aux responsabilités équivalentes.

Comité d'éthique : désigne le comité dont les membres et missions sont explicitées au chapitre IV.2 de la présente procédure.

Corruption : voir le chapitre IV du Code.

Direction : désigne tout membre de l'encadrement d'une Entité, c'est-à-dire ayant un niveau de Directeur dans l'organisation d'Exail et/ou faisant statutairement partie d'un organe de gouvernance d'une Entité.

Entité : désigne indistinctement Exail Holding SAS et/ou toute société contrôlée (directement ou indirectement) par celle-ci, en France comme à l'étranger, mais aussi les établissements secondaires et autres bureaux de ces sociétés.

Exail ou groupe Exail : désigne, collectivement, l'ensemble constitué de toutes les Entités.

Loi Sapin II : désigne la 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, révisée par la loi n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte, dite loi Wasserman, ayant donné lieu au décret n° 2022-1284 du 3 octobre 2022 relatif aux procédures de recueil et de traitement des signalements émis par les lanceurs d'alerte.

Référents : désigne les référents internes chargés du recueil et du traitement des alertes, comme explicité au chapitre IV.1 de la présente procédure.

Règlement RGPD ou RGPD : désigne le Règlement (UE) 2016/679 du parlement et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Trade Compliance Committee ou TCC : désigne le comité dont les membres et missions sont explicitées au chapitre IV.3 de la présente procédure.

II. CADRE DU DISPOSITIF D'ALERTE INTERNE

Comme explicité en détail dans le *Mémo sur la protection des lanceurs d'alerte en France*, annexe de la présente procédure, la Loi Sapin II impose de mettre en place un **dispositif d'alerte interne** au sein de certaines sociétés et groupes de sociétés :

- les articles 6 à 16 imposent de mettre en place un dispositif de protection des lanceurs d'alerte, qui doit être formalisé dans une procédure de recueil et de traitement des signalements pour ce qui concerne les signalements dits internes ;
- l'article 17 impose de mettre en œuvre « *un dispositif d'alerte interne destiné à permettre le recueil des signalements émanant d'employés et relatifs à l'existence de conduites contraires au code de conduite de la société* ».

Conformément à l'article 5 du décret n° 2022-1294 du 3 octobre 2022 et aux Recommandations de l'AFA, il est possible de mettre en place un seul et unique dispositif de recueil des signalements commun aux deux dispositions.

Assujetti à ces obligations et en cohérence avec sa démarche éthique et conformité, qui vise à établir et pérenniser une culture de transparence et d'intégrité, le groupe Exail a déployé un dispositif d'alerte interne, tel qu'explicité dans la présente procédure.

Celle-ci précise donc les principes et mesures en place au sein du groupe Exail pour le **recueil et le traitement des signalements** qui seraient émis dans le cadre précité vers Exail, par les employés, les collaborateurs externes et occasionnels ainsi que par toutes autres personnes concernées selon les dispositions légales applicables en France aux lanceurs d'alerte.

Le dispositif d'alerte interne fait ainsi partie intégrante du dispositif anticorruption déployé au sein du groupe Exail conformément aux Recommandations de l'AFA. A ce titre, il vise en particulier 2 objectifs :

- d'une part, permettre à tout Collaborateur de signaler un comportement ou une situation contraire au Code, afin d'y mettre fin et, le cas échéant, de sanctionner le(s) responsable(s) ;
- d'autre part, contribuer à l'actualisation du dispositif anticorruption, en particulier sa cartographie des risques, pour renforcer les mesures permettant de prévenir et détecter la Corruption.

A noter que dans toute la suite de la procédure et de ses annexes, on utilisera indifféremment les termes « signalement » et « alerte » avec la même signification.

La présente procédure est complétée par les documents suivants, qui en constituent des annexes :

- le *Mémo sur la protection des lanceurs d'alerte en France* ;
- le *Guide sur le dispositif ethicorp* ;
- le *Manuel utilisateur ethicorp* ;
- la *Liste des Référents* (usage interne seul) ;
- le modèle de *Charte éthique* (usage interne seul).

III. CHAMP D'APPLICATION DU DISPOSITIF

III.1. Objets d'un signalement interne

Le dispositif d'alerte interne concerne tout signalement vers Exail portant sur :

- un crime ou un délit ;
- une menace ou un préjudice pour l'intérêt général ;
- une violation ou une tentative de dissimulation d'une violation :
 - d'un engagement international régulièrement ratifié ou approuvé par la France ; ou
 - d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement ; ou
 - du droit de l'Union européenne, de la loi ou du règlement ;
- un manquement au *Code de conduite anticorruption* d'Exail ;
- un manquement à tout autre code ou charte en vigueur au sein de toute Entité et formellement intégré au règlement intérieur (en France) ou à tout autre document de portée équivalente (à l'étranger) de celle-ci.

L'alerte peut porter sur des faits qui se sont produits ou qui sont très susceptibles de se produire.

En revanche, les faits, informations et documents, quel que soit leur forme ou leur support, dont la révélation ou la divulgation est interdite par les dispositions relatives au secret de la défense nationale, au secret médical, au secret des délibérations judiciaires, au secret de l'enquête ou de l'instruction judiciaires ou au secret professionnel de l'avocat sont exclus du régime de l'alerte.

III.2. Entités concernées

Sous réserve des obligations légales de consultation des instances de dialogue social, le dispositif d'alerte interne est applicable à toutes les Entités établies en France et, sous réserve des dispositions légales et réglementaires applicables localement, à toutes les Entités établies à l'étranger.

III.3. Personnes concernées

Pour ce qui concerne le signalement interne de tout comportement ou situation contraire au Code, le dispositif d'alerte interne est applicable à tout Collaborateur.

En ce qui concerne plus généralement le dispositif légal de protection des lanceurs d'alerte applicable en France, celui doit, pour relever dudit dispositif :

- être une personne physique ;
- agir sans attendre de contrepartie financière directe ;
- être de bonne foi ;
- faire partie des personnes suivantes :
 - membres du personnel de chaque Entité ;
 - personnes dont la relation de travail s'est terminée avec une Entité, lorsque les informations ont été obtenues dans le cadre de cette relation ;

- personnes qui se sont portées candidates à un emploi au sein d'une Entité, lorsque les informations ont été obtenues dans le cadre de cette candidature ;
- actionnaires, associés et titulaires de droits de vote au sein de l'assemblée générale d'une Entité ;
- membres de l'organe d'administration, de direction ou de surveillance d'une Entité ;
- collaborateurs extérieurs et occasionnels de chaque Entité ;
- cocontractants de chaque Entité, ainsi que leurs propres sous-traitants et, lorsqu'il s'agit de personnes morales, les membres de l'organe d'administration, de direction ou de surveillance de ces cocontractants et de leurs sous-traitants ;
- membres du personnel desdits cocontractants et de leurs sous-traitants.

De plus, lorsque les informations ont bien été obtenues dans le cadre des activités professionnelles, le lanceur d'alerte peut ne pas en avoir eu personnellement connaissance, c'est-à-dire ne pas avoir été le témoin personnel ou la victime des faits. Cela ne serait par contre pas vrai dans un contexte non professionnel.

Le périmètre des personnes pouvant bénéficier du dispositif légal de protection des lanceurs d'alerte applicable en France est donc plus large que celui des seuls Collaborateurs.

L'auteur d'un signalement ne doit enfin pas agir de façon malveillante ou par vengeance en rapportant des informations qu'il sait mensongères ou erronées.

C'est à ces conditions que le lanceur d'alerte bénéficiera des pléines protections garanties par la loi (voir chapitres VIII et suivants infra). À défaut, en cas notamment de mauvaise foi, de colportage de rumeurs ou de faits diffamatoires, il ou elle s'exposera à des sanctions (voir chapitre XIII infra).

A noter qu'en ce qui concerne l'ensemble des personnes listées ci-dessus qui ne seraient pas des Collaborateurs, il incombe et reste de la responsabilité des cocontractants d'Exail de les informer du dispositif d'alerte interne en place, sur la base des informations mises à leur disposition par Exail (voir chapitre XIV infra).

III.4. Canaux de signalement et divulgation

Comme explicité au chapitre IV du *Mémo sur la protection des lanceurs d'alerte en France*, un lanceur d'alerte dispose de trois canaux distincts pour effectuer son signalement tout en bénéficiant des protections accordées par la loi à ce statut :

- le signalement interne ;
- le signalement externe ;
- la divulgation publique.

Le dispositif d'alerte interne du groupe Exail, objet de la présente procédure, ne couvre dans ce cadre que le canal du **signalement interne**. Par signalement ou alerte on entendra donc ici exclusivement un signalement ou une alerte à destination d'Exail.

Pour les dispositions relatives aux autres canaux, il convient de se référer aux dispositions légales et réglementaires applicables, telles que rappelées par exemple dans le *Mémo sur la protection des lanceurs d'alerte en France* (en particulier le chapitre IV).

IV. RÉFÉRENTS ET COMITÉS

IV.1. Référents

Les Référents impliqués dans le dispositif d'alerte interne ont pour missions, selon le découpage fonctionnel explicité ci-après, de :

- recueillir les alertes qui leurs seraient adressées directement et/ou indirectement, y compris via un canal hiérarchique interne (voir chapitres V.1, V.3 et VI infra) ;
- recevoir les alertes issues d'une transmission via le dispositif ethicorp selon les dispositions mises en place (voir chapitre V.4 infra) ;
- traiter les alertes (voir chapitre VII infra) ;
- convoquer ou impliquer, le cas échéant, le Comité d'éthique (voir chapitres IV.2) ou le TCC (voir chapitres IV.3) ;
- contribuer au reporting annuel statistique concernant la réception, le traitement ainsi que les suites données aux alertes reçues ainsi qu'à la mise à jour comme de besoin du dispositif d'alerte interne, tel que piloté par le Directeur Conformité.

Compte tenu de la structure, de la taille et de l'organisation d'Exail, il a été décidé de désigner les personnes dont les fonctions sont présentées dans le tableau ci-dessous comme Référents.

Ces personnes disposent, par leur positionnement ou leur statut, de la compétence, de l'autorité ou de la légitimité, ainsi que des moyens suffisants à l'exercice de leurs missions. La Direction Générale d'Exail assure leur indépendance dans la conduite desdites missions.

Domaine fonctionnel	Référents
Référents Ressources Humaines	<ul style="list-style-type: none"> - Directrice RH Groupe - Directrices RH des Pôles - Référents harcèlement sexuel et agissements sexistes des Entités désignés par la Direction et/ou le CSE
Référents Juridique & Conformité	<ul style="list-style-type: none"> - Directeur Juridique Groupe - Directeur Conformité Groupe

Tableau 1 – Liste fonctionnelle des Référents

Les coordonnées à jour des Référents sont précisées dans la *Liste des Référents*, accessible aux seuls Collaborateurs.

Les Référents sont tous signataires de la *Charte éthique*, qui stipule en particulier les engagements renforcés de confidentialité, d'intégrité et d'impartialité qu'ils ou elles s'engagent à respecter en toutes circonstances en lien avec la mise en œuvre du dispositif d'alerte interne.

IV.2. Comité d'éthique

Sur sollicitation d'au-moins un des Référents Ressources Humaines, un Comité d'éthique sera constitué sans délai pour procéder au traitement d'une alerte relevant de ce domaine (voir chapitre VII infra).

A noter que la constitution d'un Comité d'éthique n'est pas systématique, il incombe au(x) Référent(s) Ressources Humaines impliqué(s) de décider de l'opportunité et du moment de sa constitution, au regard du contexte du signalement et en premier lieu de la gravité des faits.

En l'absence de constitution d'un Comité d'éthique, le(s) Référent(s) en charge du traitement assure(nt) directement le déroulé de celui-ci (voir chapitre VII infra).

Un Comité d'éthique peut être constitué dès la réception du signalement par le(s) Référent(s) concerné(s) ou a posteriori selon les besoins. Une fois constitué et sous réserve que le signalement ne soit pas a posteriori déclaré sans objet, un Comité d'éthique constitué assurera le traitement dudit signalement jusqu'à sa clôture.

Un Comité d'éthique est composé :

- d'au-moins un membre du CODIR d'Exail ;
- de la Directrice RH Groupe ;
- de l'un ou des autres Référents RH (y compris les Référents harcèlement sexuel et agissements sexistes), en particulier quand le signalement est en lien avec leur rattachement organisationnel ;
- des Référents Juridique & Conformité comme de besoin ;
- de toute autre personne dont la participation serait nécessaire.

La composition d'un Comité d'éthique est validée par le ou les membres du CODIR d'Exail qui y siègent et la Directrice RH Groupe.

Afin de garantir l'impartialité du dispositif d'alerte interne, aucune personne ne pourra faire partie d'un Comité d'éthique si elle est impliquée dans le signalement et/ou en conflit d'intérêt personnel avéré dans le cadre de celui-ci.

Les membres d'un Comité d'éthique sont tous signataires de la *Charte éthique*, qui stipule en particulier les engagements renforcés de confidentialité, d'intégrité et d'impartialité qu'ils ou elles s'engagent à respecter en toutes circonstances en lien avec la mise en œuvre du dispositif d'alerte interne.

IV.3. Trade Compliance Committee (TCC)

Le Trade Compliance Committee ou TCC est un comité permanent mis en place au sein d'Exail dans le cadre du dispositif de prévention et détection de la corruption.

Il a pour principales missions : (i) de traiter les dossiers d'évaluation des tiers qui lui sont adressés selon la *Procédure d'évaluation des tiers* du groupe Exail, (ii) d'examiner et traiter toute alerte qui lui est adressée par les Référents Juridique & Conformité, en

particulier en ce qui concerne les atteintes au Code, (iii) de suivre et superviser la bonne mise en œuvre du dispositif de prévention et détection de la corruption, y compris le dispositif d'alerte interne, et (iv) de prendre toute mesure nécessaire relative à l'efficacité dudit dispositif, y compris le dispositif d'alerte interne.

Le TCC est composé :

- des membres du CODIR d'Exail ;
- des Directeurs Juridique & Conformité ;
- des Directeurs Commerciaux Groupe.

En cohérence avec les Recommandations de l'AFA, tout signalement relatif (i) à des faits susceptibles de constituer des violations du Code, (ii) à des comportements non conformes aux procédures internes visant à prévenir ou à détecter la commission de telles violations ou (iii) à des indices de la commission de faits susceptibles d'être qualifiés de Corruption, sera systématiquement et immédiatement adressé par les Référénts concernés au TCC, qui en assurera le traitement (voir chapitre VII infra).

Pour tout autre signalement reçu par les Référénts Juridique & Conformité l'implication du TCC n'est en revanche pas systématique. Il incombe auxdits Référénts de décider de l'opportunité de l'implication directe du TCC dans le traitement du signalement, au regard du contexte de celui-ci et en premier lieu de la gravité des faits. Dans un tel cas, le TCC peut être impliqué dès la réception du signalement par les Référénts concernés ou a posteriori selon les besoins. Une fois impliqué et sous réserve que le signalement ne soit pas a posteriori déclaré sans objet, le TCC assurera le traitement dudit signalement jusqu'à sa clôture (voir chapitre VII infra).

En l'absence d'implication directe du TCC, le(s) Référént(s) en charge du traitement assure(nt) directement le déroulé de celui-ci (voir chapitre VII infra).

Afin de garantir l'impartialité du dispositif d'alerte interne, aucune personne ne pourra participer aux travaux du TCC en lien avec un signalement qui lui a été adressé si elle est impliquée dans ledit signalement et/ou en conflit d'intérêt personnel avéré dans le cadre de celui-ci.

Les membres du TCC sont tous signataires de la *Charte éthique*, qui stipule en particulier les engagements renforcés de confidentialité, d'intégrité et d'impartialité qu'il ou elle s'engage à respecter en toutes circonstances en lien avec la mise en œuvre du dispositif d'alerte interne.

V. COMMENT LANCER UNE ALERTE

V.1. Sollicitation du canal hiérarchique

Avant de lancer une alerte, tout Collaborateur pourra, s'il le souhaite, s'adresser à son supérieur hiérarchique, responsable ou tuteur, direct ou indirect, ce dernier ayant pour devoir de l'assister et l'orienter comme de besoin (voir aussi chapitre XIV infra).

Cependant, si le Collaborateur confirme son souhait de déposer une alerte, il conviendra de l'orienter **sans délai** vers le dispositif ethicorp ou un Référent, **seuls** autorisés à recueillir un signalement pour garantir l'intégrité de la démarche, dans le respect des obligations légales et réglementaires applicables (voir en particulier le chapitre VIII).

V.2. Canaux disponibles pour l'envoi d'une alerte

Afin de garantir la plus grande efficacité au dispositif d'alerte interne, dans le respect des obligations d'intégrité, de confidentialité et d'impartialité, deux canaux distincts peuvent être utilisés par toute personne concernée pour adresser un signalement :

1. Contacter les **Référents** internes comme explicité au chapitre V.3 infra.
2. Utiliser le dispositif externalisé **ethicorp** comme explicité au chapitre V.4 infra.

A noter que le dispositif d'alerte ethicorp n'est qu'un des deux moyens de signalement utilisables, le fait de ne pas y avoir recours ne peut entraîner aucune sanction à l'encontre des Collaborateurs.

Le contenu d'une alerte et les autres dispositions communes aux deux canaux de signalement sont explicités au chapitre V.5 infra.

V.3. Envoi d'une alerte directement aux Référents

Les Référents peuvent être contactés directement pour transmettre une alerte via les adresses mail fonctionnelles suivantes, partagées par les Référents concernés selon les domaines fonctionnels associés :

- alert.hr@exail.com pour tous les sujets relevant des ressources humaines ;
- alert.compliance@exail.com pour tous les autres sujets.

Toute alerte émise via ce canal doit être formulée en français ou en anglais.

Afin de garantir l'efficacité, l'intégrité et la robustesse du dispositif d'alerte interne quand les Référents sont directement contactés, il est recommandé d'utiliser ces adresses fonctionnelles partagées plutôt que leurs adresses personnelles.

En revanche, ces adresses fonctionnelles étant partagées par les Référents, au cas où l'un d'entre eux serait personnellement concerné par une alerte, il est préférable d'utiliser le dispositif ethicorp pour éviter toute situation de conflit d'intérêt.

Enfin, au cas où un Collaborateur souhaiterait impérativement contacter un Référent sans passer par messagerie, il ou elle peut le faire en s'appuyant sur la *Liste des Référents*. Le signalement pourra alors être recueilli par téléphone ou, sur demande du Collaborateur

et selon son choix, lors d'une visioconférence ou d'une rencontre physique organisée au plus tard vingt jours ouvrés après réception de la demande. Dans ce cas, les modalités de consignation de l'alerte seront définies au préalable de celle-ci de façon à garantir le respect des obligations légales spécifiques associées à un signalement oral.

V.4. Envoi d'une alerte via le dispositif ethicorp

Exail a souscrit au dispositif d'alerte **ethicorp**, permettant d'apporter les plus hautes garanties d'impartialité et d'indépendance aux personnes qui souhaiteraient l'utiliser pour déposer une alerte.

La plateforme **ethicorp** est accessible par internet à l'adresse sécurisée <https://www.ethicorp.org>.

Cette plateforme française de réception et pré-traitement des alertes est entièrement gérée et administrée par des avocats, professionnels réglementés indépendants, astreints à des obligations déontologiques et disciplinaires strictes, notamment en matière de confidentialité et secret professionnel.

ethicorp dispose ainsi, par son positionnement, de la compétence, de l'autorité et des moyens suffisants à l'exercice de ses missions.

L'utilisation du dispositif **ethicorp** est décrit en détail dans les documents suivants, constituant des annexes de la présente procédure :

- le *Guide sur le dispositif ethicorp* ;
- le *Manuel utilisateur ethicorp*.

On retrouve en particulier dans le *Guide sur le dispositif ethicorp* les codes corporate associés à Exail nécessaires à la création d'un compte sur la plateforme, étape préalable au dépôt d'une alerte.

V.5. Contenu d'une alerte et autres dispositions communes

Quel que soit le canal utilisé, l'alerte doit comporter :

- l'identité, les coordonnées (y compris une adresse de messagerie valide) et, idéalement, la situation professionnelle de l'émetteur de l'alerte, sauf s'il choisit de rester anonyme, dans les conditions explicitées ci-dessous ;
- les faits qu'il souhaite rapporter, avec un niveau de détail approprié ;
- les informations, documents et autres éléments de nature à étayer le signalement, lorsqu'il dispose de tels éléments.

Lorsque des éléments en support du signalement ne pourraient être transmis par voie de messagerie, des modalités appropriées de recueil seront définies au cas par cas avec le destinataire du signalement.

Pour éviter toute question au regard de la confidentialité, il est recommandé de ne pas utiliser le matériel de son entreprise pour se connecter. De même, il est recommandé,

toujours pour des questions de confidentialité, de ne pas utiliser une adresse électronique professionnelle.

En accord avec la recommandation de la CNIL de juillet 2019, Exail n'incite pas les personnes ayant vocation à utiliser le dispositif à le faire de manière anonyme. Quoi qu'il en soit, son identité sera en effet toujours traitée de manière confidentielle (voir chapitre VIII infra).

Par exception au principe de s'identifier, la CNIL précise que l'alerte d'une personne qui souhaite rester anonyme peut être traitée sous deux conditions cumulatives :

- la gravité des faits mentionnés est établie et les faits suffisamment détaillés, il sera donc indispensable d'être précis dans le descriptif des faits ;
- le traitement de l'alerte s'entoure de précautions particulières, notamment un examen préalable par son premier destinataire de l'opportunité de sa diffusion.

Si ces conditions ne sont pas réunies, le destinataire de l'alerte pourra informer le lanceur d'alerte qu'il ou elle doit s'identifier ou qu'à défaut l'alerte ne pourra pas être traitée.

VI. COMMENT EST RECEPTIONNÉE UNE ALERTE

VI.1. Accusé-réception

Quel que soit le canal utilisé, un accusé-réception écrit est envoyé par le destinataire de l'alerte dans un délai de sept jours ouvrés à compter de la réception du signalement, sauf en cas de signalement anonyme qui n'aurait pas été rejeté et pour lequel il ne serait matériellement pas possible de contacter l'auteur de celui-ci.

A noter que cet accusé-réception ne vaut pas recevabilité du signalement.

VI.2. Recevabilité

Quel que soit le canal utilisé, le destinataire de l'alerte procède sans tarder à une première analyse de celle-ci afin d'évaluer le sérieux, la pertinence, la nature et la gravité des faits allégués.

Par ailleurs, sauf en cas de signalement anonyme qui n'aurait pas été rejeté, le destinataire de l'alerte vérifie que les conditions d'éligibilité au dispositif légal de protection des lanceurs d'alerte sont respectées (voir chapitres III.1 et III.3 supra).

Afin de confirmer la recevabilité de l'alerte, tout complément nécessaire d'information pourra être demandé à l'auteur du signalement, selon le canal utilisé, sauf en cas de signalement anonyme pour lequel il ne serait matériellement pas possible de contacter celui-ci.

L'auteur du signalement sera informé des raisons pour lesquelles le destinataire de l'alerte estime, le cas échéant, que son signalement ne respecte pas les conditions d'éligibilité. Il sera également informé dans ce cadre si son signalement est rejeté ou s'il va quand même faire l'objet d'un traitement.

A l'issue de l'analyse de recevabilité de l'alerte, si celle-ci apparaît fondée elle fait l'objet d'un traitement approprié (voir chapitre VII infra).

Dans le cas d'utilisation du canal ethicorp, après confirmation de la recevabilité de l'alerte comme explicité ci-avant, l'alerte est transmise via une note de synthèse aux Référents concernés (voir chapitre II du *Guide sur le dispositif ethicorp*).

A contrario, si cette première analyse montre clairement le caractère inexact ou infondé de l'alerte, celle-ci est immédiatement classée sans suite et clôturée. L'auteur du signalement est informé de la clôture de l'alerte quand celle-ci est ainsi classée sans suite.

VII. COMMENT EST TRAITÉE UNE ALERTE

VII.1. Prise en charge

Suite à la réception d'une alerte recevable, quel que soit le canal utilisé, l'un au-moins des Référents concernés prend en charge son traitement.

En cas de constitution d'un Comité d'éthique (voir chapitre IV.2 supra) ou d'implication du TCC (voir chapitre IV.3 supra), le traitement du signalement est piloté au niveau dudit Comité d'éthique ou du TCC.

VII.2. Confirmation du traitement

Le cas échéant, si les informations disponibles à ce stade ne permettent pas de statuer clairement sur le caractère fondé de l'alerte, il sera procédé à des investigations complémentaires pour confirmer l'opportunité de poursuivre le traitement.

A ce titre, tout complément nécessaire d'information pourra, si possible et pertinent, être demandé à l'auteur du signalement, selon le canal utilisé.

Si ces investigations montrent le caractère inexact ou infondé de l'alerte, celle-ci est classée sans suite et clôturée. A contrario, si ces investigations confirment le caractère fondé de l'alerte, le traitement est poursuivi par une enquête interne.

VII.3. Enquête interne

L'enquête interne sera menée afin de déterminer précisément l'exactitude et la matérialité des faits rapportés dans le signalement. Elle sera effectuée de manière exhaustive, impartiale, confidentielle et contradictoire.

Dans ce cadre, tout complément nécessaire d'information pourra, si possible et pertinent, être demandé à l'auteur du signalement, selon le canal utilisé.

Dans le respect des dispositions légales et réglementaires applicables, en particulier en ce qui concerne la confidentialité, la présomption d'innocence et les droits de la défense (voir chapitre X infra), des entretiens pourront être menés comme de nécessaire avec (i) la ou les personnes objet de l'alerte, (ii) les éventuels tiers identifiés dans le signalement et (iii) toute personne qu'il conviendrait d'entendre pour l'efficacité de l'enquête interne.

L'ensemble des entretiens menés feront l'objet de comptes-rendus écrits formalisés de manière appropriée.

Comme de besoin, il pourra également être fait appel dans le cadre de l'enquête interne à des ressources internes et/ou externes dont l'expertise serait nécessaire au traitement de celle-ci. Ces personnes signeront au préalable la *Charte éthique* ou tout document équivalent, stipulant en particulier les engagements renforcés de confidentialité, d'intégrité et d'impartialité qu'elles s'engagent à respecter en toutes circonstances en lien avec leur implication dans l'enquête interne.

A l'issue de l'enquête interne, une note ou un rapport de synthèse (selon la nature, la gravité et l'étendue des faits) sera rédigé, annexant toutes les pièces justificatives appropriées.

VII.4. Suites données

Une fois l'enquête interne terminée et sur la base de la note ou du rapport de synthèse, les suites données au signalement seront formellement décidées puis mises en œuvre par les personnes ayant autorité pour le faire, pour chaque Entité concernée, à savoir :

- les mesures à prendre pour, le cas échéant, remédier à l'objet du signalement ;
- l'éventuelle mise en œuvre d'une procédure disciplinaire et/ou le lancement d'une action en justice ;
- les éventuelles autres suites à donner en lien avec :
 - le fonctionnement et/ou l'organisation de toute Entité concernée ;
 - tout élément du dispositif anticorruption d'Exail, y compris le dispositif d'alerte interne ;
 - tout autre élément pertinent (par exemple règlement intérieur, chartes et codes, procédures, notes de service ...).

Une fois l'ensemble des actions formellement décidées, l'alerte est clôturée.

VII.5. Information de l'auteur du signalement

Sauf en cas de signalement anonyme pour lequel il ne serait matériellement pas possible de contacter l'auteur de celui-ci, un retour écrit est fait a minima à l'auteur du signalement, selon le canal utilisé, comme suit :

- Dans un délai raisonnable n'excédant pas trois mois à compter de l'accusé-réception du signalement ou, à défaut d'accusé-réception, trois mois à compter de l'expiration d'une période de sept jours ouvrés suivant le signalement, l'auteur de celui-ci est informé sur les mesures envisagées ou prises pour évaluer l'exactitude des allégations et, le cas échéant, remédier à l'objet du signalement, ainsi que les motifs desdites mesures.
- L'auteur du signalement est informé de la clôture de l'alerte, y compris si celle-ci est finalement classée sans suite.

VIII. CONFIDENTIALITÉ

Conformément à l'article 9 de la Loi Sapin II, doivent demeurer strictement confidentielles :

- l'identité du lanceur d'alerte, qui doit pouvoir ainsi déposer son alerte en toute tranquillité ;
- l'identité de la personne visée par l'alerte et celle de tout tiers mentionné dans le signalement ;
- les informations recueillies dans le cadre de l'alerte, c'est à dire les faits objets de l'alerte.

Ces deux derniers éléments (identité de la personne visée et de tout tiers mentionné dans le signalement et informations recueillies dans le cadre de l'alerte) ne seront en pratique connus que des personnes chargées du recueil puis du traitement de l'alerte, pour les besoins de celle-ci et avec une stricte obligation de confidentialité.

L'accès à ces informations est interdit aux Collaborateurs qui ne sont pas autorisés à en connaître selon les dispositions de la présente procédure. C'est pourquoi il est impératif que soient transmis sans délai aux Référénts des signalements qui auraient éventuellement été transmis directement à d'autres Collaborateurs.

Hors personnes autorisées, les éléments de nature à identifier le lanceur d'alerte ne peuvent ainsi être divulgués qu'avec le consentement de celui-ci.

Ils peuvent toutefois être communiqués à l'autorité judiciaire, dans le cas où les personnes chargées du recueil ou du traitement des signalements sont tenues de dénoncer les faits à celle-ci. Le lanceur d'alerte en est alors informé, à moins que cette information ne risque de compromettre la procédure judiciaire. Des explications écrites sont jointes à cette information.

Par ailleurs, le lanceur d'alerte ne peut pas lui-même divulguer librement les informations objet de l'alerte, sauf dans le cadre strict d'une divulgation publique (cf. chapitre III.4 supra).

IX. PROTECTION DU LANCEUR D'ALERTE

Conformément à l'article 10-1 et 12 à 13-1 de la Loi Sapin II révisée, le lanceur d'alerte bénéficie d'une **protection contre toute mesure de rétorsion**.

Il est par exemple rappelé qu'aucune personne ne peut être écartée d'une procédure de recrutement, de l'accès à un stage ou à une période de formation professionnelle, aucun salarié ne peut être sanctionné, licencié ou faire l'objet d'une mesure discriminatoire, pour avoir signalé une alerte (cf. chapitre VII du *Mémo sur la protection des lanceurs d'alerte en France*)

Les mesures de rétorsion contre un lanceur d'alerte constituent par ailleurs un délit de discrimination, conformément à l'article 225-1 du Code pénal (voir également le chapitre XIII infra pour les sanctions associées).

Le lanceur d'alerte bénéficie également, dans certains cas et à certaines conditions, d'une irresponsabilité pénale et civile.

Cette protection ne s'applique bien sûr que si le lanceur d'alerte respecte le cadre prévu par les articles 6 à 8 de la Loi Sapin II.

A contrario, le lanceur d'alerte ne sera pas protégé s'il ne répond pas aux définitions légales et notamment s'il déclare des faits de mauvaise foi et/ou dont il n'aurait pas eu personnellement connaissance lorsque les informations n'ont pas été obtenues dans le cadre de son activité professionnelle.

Ceci rappelé, l'utilisation **de bonne foi** du dispositif n'exposera son auteur à aucune sanction disciplinaire, quand bien même les faits s'avèreraient par la suite inexacts ou ne donneraient lieu à aucune suite.

X. DROITS DES PERSONNES VISÉES PAR UNE ALERTE

Toute personne visée par une alerte a droit au respect de sa stricte confidentialité, notamment au regard du principe fondamental de sa présomption d'innocence et de ses droits de la défense. Les éléments de nature à l'identifier ne peuvent être divulgués, sauf à l'autorité judiciaire, qu'une fois établi le caractère fondé de l'alerte.

La personne qui fait l'objet d'une alerte (en tant que témoin, victime ou auteur présumé des faits) doit, conformément à l'article 14 du RGPD, être informée dans un délai raisonnable, **ne pouvant pas dépasser un mois**, à la suite de l'émission d'une alerte.

Néanmoins, conformément à l'article 14-5-b du RGPD, cette information peut être différée lorsqu'elle est susceptible « *de compromettre gravement la réalisation des objectifs dudit traitement* ». Tel pourrait, par exemple, être le cas lorsque la divulgation de ces informations à la personne visée compromettrait gravement les nécessités d'une enquête, par exemple en présence d'un risque de destruction de preuves. L'information doit néanmoins alors être délivrée aussitôt le risque écarté et ne doit pas contenir d'informations relatives à l'identité de l'émetteur de l'alerte, ni à celle des tiers.

De même, l'enquête interne diligentée suite à la dénonciation de faits de harcèlement moral n'impose pas obligatoirement à l'employeur de donner au salarié accusé l'accès au dossier. La Cour de cassation affirme dans un arrêt de juin 2022 que le respect des droits de la défense et du principe de la contradiction n'impose pas notamment que, dans le cadre d'une enquête interne destinée à vérifier la véracité des agissements dénoncés par d'autres salariés, le salarié incriminé ait accès au dossier et aux pièces recueillies ou qu'il soit confronté aux collègues qui le mettent en cause.

Toutefois, lorsqu'une procédure contentieuse est engagée à la suite de l'alerte à l'égard de la personne visée, celle-ci peut obtenir la communication de ces éléments en vertu des règles de droit commun (droits de la défense notamment).

Cette possibilité est néanmoins conditionnée à la prise de mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes de toute personne concernée.

XI. TRAITEMENT DES DONNÉES PERSONNELLES

Toute donnée personnelle communiquée en application du dispositif d'alerte interne sera traitée conformément aux dispositions légales et réglementaires applicables en matière de protection et traitement des données à caractère personnel (cf. chapitre IX du *Mémo sur la protection des lanceurs d'alerte en France*).

Les données personnelles collectées et traitées dans le cadre d'une alerte le sont dans le seul but de se conformer aux obligations de la Loi Sapin II et, plus généralement, aux obligations légales et réglementaires applicables à Exail. En particulier, seules les données personnelles nécessaires à la poursuite des finalités du traitement associé seront effectivement collectées et traitées.

Elles seront enregistrées dans un fichier informatisé et pourront être transmises comme de besoin aux personnes impliquées dans le recueil et le traitement des alertes ainsi que, le cas échéant, aux autorités administratives et judiciaires, toujours dans le respect des dispositions légales et réglementaires applicables.

Les personnes concernées par une alerte disposent des droits suivants en ce qui concerne leurs données personnelles, qu'ils ou elles exercent dans les conditions prévues par le RGPD :

- droit de s'opposer au traitement de leurs données, sous réserve des conditions d'exercice de ce droit en application des dispositions de l'article 21 du RGPD (le droit d'opposition ne peut ainsi pas être exercé pour les traitements nécessaires au respect d'une obligation légale à laquelle est soumis le responsable du traitement, notamment concernant les traitements mis en place et remplissant les conditions des articles 8 et/ou 17 de la Loi Sapin II) ;
- droit d'accès, de rectification (au regard de la finalité du traitement) et d'effacement des données qui les concernent ;
- droit à la limitation du traitement.

Lorsque les personnes concernées exercent leur droit d'accès, elles ne peuvent, via l'exercice de ce droit, obtenir communication d'aucune donnée relative à des tiers.

La personne visée par l'alerte qui exercerait son droit d'accès ne peut en aucun cas obtenir communication des informations concernant l'identité de l'émetteur de l'alerte.

La durée de conservation des données personnelles est encadrée par les dispositions exposées au chapitre XII infra.

Pour toute demande relative au traitement des données personnelles via le dispositif d'alerte interne, s'adresser au Directeur Conformité (voir chapitres IV.1 supra ou XIV infra).

XII. CONSERVATION ET DESTRUCTION DES DONNÉES

La conservation des données à caractère personnel est soumise aux dispositions de la loi du 6 janvier 1978 et du RGPD, en vigueur depuis le 25 mai 2018. Notamment, les données à caractère personnel ne peuvent être conservées que le temps strictement nécessaire à l'accomplissement de la finalité pour laquelle elles ont été collectées.

L'article 9-III de la Loi Sapin II révisée prévoit également que : « *Les signalements ne peuvent être conservés que le temps strictement nécessaire et proportionné à leur traitement et à la protection de leurs auteurs, des personnes qu'ils visent et des tiers qu'ils mentionnent, en tenant compte des délais d'éventuelles enquêtes complémentaires.* »

Conformément au point 7.1 du référentiel établi par la CNIL dans sa délibération du 18 juillet 2019, les données relatives à une alerte seront donc gérées comme suit :

- Les données relatives à une alerte considérée comme n'entrant pas dans le champ du dispositif sont détruites **sans délai**.
- Lorsqu'aucune suite¹ n'est donnée à une alerte rentrant dans le champ du dispositif, les données relatives à cette alerte sont détruites ou anonymisées dans un délai de **deux mois** à compter de la clôture des opérations de vérification.
- Lorsqu'une suite¹ est donnée à l'alerte, hors procédure disciplinaire ou contentieuse, les données relatives à l'alerte pourront être conservées sous forme d'archives intermédiaires aux fins d'assurer la protection du lanceur de l'alerte ou de permettre la constatation des infractions continues. Cette durée de conservation doit être strictement limitée aux finalités poursuivies, déterminée à l'avance au cas par cas et portée à la connaissance des personnes concernées.
- Lorsqu'une procédure disciplinaire ou contentieuse est engagée à l'encontre d'une personne mise en cause ou de l'auteur d'une alerte abusive, les données relatives à l'alerte peuvent être conservées **jusqu'au terme de la procédure ou de la prescription des recours à l'encontre de la décision**.
- Enfin, les données peuvent toujours être conservées plus longtemps, en archivage intermédiaire, si le responsable du traitement en a l'obligation légale (par exemple, pour répondre à des obligations comptables, sociales ou fiscales).

Pour plus d'information, se reporter au chapitre IX.2 du *Mémo sur la protection des lanceurs d'alerte en France*.

¹ Conformément au référentiel de la CNIL du 18 juillet 2019 l'expression « *suites* » désigne toute décision prise par l'organisme pour tirer des conséquences de l'alerte. Il peut s'agir de l'adoption ou de la modification des règles internes (règlement interne, charte éthique, etc.) de l'organisme, d'une réorganisation des opérations ou des services de la société, du prononcé d'une sanction ou de la mise en œuvre d'une action en justice.

XIII. SANCTIONS

Toute mesure de représailles, directes ou indirectes, à l'encontre d'un Collaborateur qui a signalé une alerte ne saurait être tolérée et donnera lieu à des sanctions disciplinaires pouvant aller jusqu'à la rupture du contrat de travail, conformément au droit applicable.

La Loi Sapin II prévoit également que toute personne qui fait obstacle, de quelque façon que ce soit, à la transmission d'une alerte est punie d'un an d'emprisonnement et 15 000 euros d'amende (75 000 euros pour les personnes morales).

Par ailleurs, l'utilisation abusive du dispositif d'alerte interne peut exposer son auteur à des sanctions disciplinaires et/ou des sanctions judiciaires, civiles et pénales, notamment pour diffamation ou dénonciation calomnieuse.

Enfin, toute violation de la confidentialité de l'alerte pourra également donner lieu à des sanctions disciplinaires pouvant aller jusqu'à la rupture du contrat de travail, conformément au droit applicable.

Cette violation est également punie de deux ans d'emprisonnement et 30 000 euros d'amende (150 000 euros pour les personnes morales).

L'ensemble des sanctions seront appliquées conformément :

- aux stipulations du règlement intérieur (en France) ou de tout autre texte équivalent (à l'étranger) de la société dont relève la personne concernée ; et/ou
- aux dispositions légales et réglementaires applicables en la matière.

XIV. INFORMATION ET SENSIBILISATION

La présente procédure est :

- intégrée dans les règlements intérieurs (en France) et dans les documents équivalents localement (à l'étranger) des Entités ;
- disponible publiquement sur le(s) site(s) internet d'Exail ;
- mentionnée dans les CGA, les CGV et les clauses contractuelles d'Exail ;
- évoquée dans le *Code de conduite fournisseur et partenaire* d'Exail ;
- disponible pour les Collaborateurs sur les intranet(s) d'Exail ;
- communiquée à l'ensemble des Collaborateurs à l'occasion de sa diffusion initiale comme de toute modification significative ;
- communiquée à chaque nouveau Collaborateur d'Exail ;
- présentée aux Collaborateurs, en particulier tout nouveau Collaborateur d'Exail, dans le cadre des actions de sensibilisation de l'ensemble des personnels.

Tout Collaborateur ayant besoin d'aide concernant l'interprétation de l'une quelconque des stipulations de la présente procédure peut s'adresser :

- à son responsable ;
- au Service Ressources Humaines de l'Entité dont il dépend ;
- à la Direction Juridique & Conformité, par exemple via les adresses legal@exail.com ou compliance@exail.com ;
- directement à l'un des Référents (voir chapitre IV.1 supra).

XV. A RETENIR

Comme décrit au chapitre II, le dispositif d'alerte interne d'Exail est instauré en application des dispositions légales et réglementaires applicables en France, en particulier la Loi Sapin II. Il fait partie intégrante du dispositif anticorruption déployé au sein du groupe Exail conformément aux Recommandations de l'AFA.

Si le dispositif doit être connu, compris et interprété dans son intégralité, il s'articule autour de **six points principaux** :

1. Le dispositif précise le champ d'application et les conditions du régime légal des alertes, en particulier en ce qui concerne l'éligibilité au statut de lanceur d'alerte (voir chapitre III).
 - a. Il est ainsi directement applicable pour l'ensemble des Collaborateurs du groupe Exail en France.
 - b. Sous réserve des dispositions légales et réglementaires applicables localement, il est également applicable aux Collaborateurs du groupe Exail des Entités établies à l'étranger.
 - c. Il est enfin ouvert aux autres personnes concernées hors Collaborateurs d'Exail selon les conditions explicitées.
2. Une organisation interne spécifique est mise en place par le dispositif pour assurer le recueil et le traitement des signalements, via des Référents internes et des comités spécifiques (voir chapitre IV).
3. Le dispositif explicite les modalités pratiques du lancement d'une alerte (voir chapitre V), via deux canaux possibles : (i) les Référents internes ou (ii) le dispositif externalisé ethicorp.
4. Le dispositif définit les principes fondamentaux et les modalités pratiques de la réception puis du traitement d'une alerte (voir chapitres VI et VII), y compris l'information de l'auteur du signalement quant à la réception, le traitement et la clôture de l'alerte.
5. Le dispositif confirme l'ensemble des mesures spécifiques associées à une alerte, selon les dispositions légales et réglementaires applicables, en ce qui concerne :
 - a. la confidentialité (voir chapitre VIII) ;
 - b. la protection du lanceur d'alerte (voir chapitre IX) ;
 - c. les droits des personnes visées par une alerte (voir chapitre X) ;
 - d. le traitement des données personnelles (voir chapitre XI) ;
 - e. la conservation et destruction des données (voir chapitre XII).
6. Si l'utilisation de bonne foi et désintéressée du dispositif octroie a priori un régime de protection à son auteur, une alerte intentionnellement mensongère et plus généralement une utilisation abusive du dispositif peut exposer son auteur à des sanctions disciplinaires et/ou à des poursuites judiciaires (voir chapitre XIII).

XVI. ANNEXES

Les documents suivants constituent des annexes de la présente procédure :

- le *Mémo sur la protection des lanceurs d'alerte en France* ;
- le *Guide sur le dispositif ethicorp* ;
- le *Manuel utilisateur ethicorp* ;
- la *Liste des Référents* (usage interne seul);
- le modèle de *Charte éthique* (usage interne seul).