DISPOSITIF D'ALERTE INTERNE

Sommaire

1. OBJECTIFS ET CHAMP D'APPLICATION DU DISPOSITIF D'ALERTE INTERNE

1.1 UN DISPOSITIF UNIQUE D'ALERTE POUR LE RECUEIL DE DEUX TYPES DE SIGNALEMENT

Conformément à la loi Sapin 2[1], le présent dispositif répond au double objectif suivant :

1. **Recueil des alertes anti-corruption**[2] : dans le cadre de la prévention et de la détection des faits de corruption et de trafic d'influence en France et à l'étranger auxquels le groupe pourrait être confronté, chaque salarié des filiales du groupe peut signaler aux Référents anti-corruption de Exail Technologies des éventuelles conduites contraires au Code de conduite anti-corruption de Exail Technologies[3] ou le cas échéant au code de conduite anti-corruption adopté par les filiales de Exail Technologies.

2. **Recueil des alertes générales de faits très graves**[4] : tout salarié et tout collaborateur extérieurs ou occasionnels (stagiaire, intérimaire, prestataire, sous-traitant) des filiales françaises de plus de 50 salariés de Exail Technologies peut signaler des éventuels crimes, délits, violations graves et manifestes d'une réglementation internationale applicable, de lois ou règlements ou des menaces ou préjudices graves pour l'intérêt général.

Le terme « collaborateur » utilisé ci-après inclut donc tout salarié du groupe et tout collaborateur extérieur ou occasionnel.

Les filiales de Exail Technologies sont invitées à adopter ce dispositif d'alerte, si elles n'en ont pas déjà un. Il sera alors annexé à leur règlement intérieur après consultation des IRP et diffusé en interne à tous les collaborateurs, par tout moyen (affichage, envoi, intranet, etc.).

Ce dispositif est complémentaire des autres dispositifs existant le cas échéant dans les filiales du groupe. Son utilisation ne constitue qu'une faculté supplémentaire offerte à tout collaborateur.

1.2 DEFINITION D'UN LANCEUR D'ALERTE

Le statut protecteur de lanceur d'alerte sera applicable si le lanceur d'alerte respecte tous les critères suivants :

- Il est une ***personne physique*** ;
- Le lanceur d'alerte signale des faits dont il a ***personnellement connaissance*** ou qui lui ont ***été rapportés par autrui*** dans le cadre professionnel ;

[1] Loi 2016-1691 du 9 décembre 2019 dite « Loi Sapin 2 »
[2] Conformément à l'article 17 de la Loi Sapin 2
[3] Le Code de conduite anti-corruption de Exail Technologies est en ligne sur le site Internet du groupe www.exail-technologies.com
[4] Conformément à l'article 6 de la Loi Sapin 2

- Le lanceur d'alerte agit ***sans contrepartie financière directe*** : il n'est pas rémunéré par quiconque en contrepartie de sa démarche ;
- Il agit de ***bonne foi*** : au moment où il effectue un signalement, les faits signalés doivent présenter toutes les apparences d'un fait de corruption de sorte qu'a posteriori, il ne puisse être reproché au lanceur d'alerte d'avoir cherché à nuire à autrui.
  Il est à cet égard rappelé que l'auteur de fausses allégations encourt des poursuites (voir chapitre 4).
- Les faits révélés sont graves, ils constituent :
  - une violation du Code de conduite anti-corruption de Exail Technologies ou d'une des filiales de Exail Technologies
  - un crime, un délit,
  - une violation grave et manifeste d'un engagement 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, du droit de l'Union Européenne, ou
  - une menace ou un préjudice graves pour l'intérêt général, ou
  - une tentative de dissimulation des violations précitées
- Le lanceur d'alerte ne peut révéler d'informations couvertes par le secret de la Défense Nationale, le secret médical, le secret des relations entre un avocat et son client ou le secret des délibérations judiciaires, de l'enquête ou de l'instruction judiciaire.

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 (voir chapitre 4).

↘L'alerte doit être faite de bonne foi, sur la base de faits dont le lanceur d'alerte a eu personnellement connaissance ou qui lui ont été rapportés par autrui.

↘ L'alerte ne porte pas sur un conflit du travail individuel ou collectif : l'alerte a une portée générale visant le bien commun, l'éthique.

↘ L'alerte est une faculté ouverte à tout citoyen d'exercer librement sa responsabilité pour alerter sur des crimes et délits ou des risques graves pour la santé, la sécurité publique ou l'environnement ; ce n'est pas une obligation.

1.3 REFERENTS ET COMITE ETHIQUE

Le(s) Référent(s) est(sont) chargé(s) de recueillir et traiter les alertes adressées sur l'email d'alerte compliance@exail-technologies.com.

Le Président directeur général de Exail Technologies a nommé le Directeur juridique de Exail Technologies et le Directeur général adjoint Finances comme Référents. Nommer deux personnes permet de limiter les risques de retard de traitement en cas d'absence de l'un ou l'autre. Ces deux

personnes sont nommées en raison de leur compétence, autorité et les moyens suffisants dont ils disposent pour exercer correctement cette mission.

Les Référents, en fonction des signalements reçus, forment un **Comité éthique**, pour décider du traitement des signalements, mettre en œuvre une enquête et qualifier les faits. Ce Comité peut être composé de :

- le DRH de la filiale concernée
- un expert informatique interne ou externe
- des référents des autres filiales du groupe
- un avocat
- tout spécialiste interne ou externe au groupe dont l'expertise est nécessaire au traitement d'une alerte
- en cas de difficultés particulières (importance des sujets, personnes impliquées, …) une remontée à la direction générale de la filiale concernée et au PDG de Exail Technologies est organisée.

La géométrie de ce Comité éthique ainsi constitué dépendra des alertes et des expertises requises au cas par cas. Le comité ne peut comporter de personnes en position de conflit d'intérêt dans le cadre d'une alerte donnée.

Chaque membre du Comité éthique sera amené à signer une charte éthique qui rappellera (i) les principes généraux régissant les alertes internes, (ii) les modalités de conduite des enquêtes internes, (iii) les obligations de confidentialité, neutralité et d'impartialité à respecter en toutes circonstances par les membres du Comité.

Le Comité éthique traitera les alertes transmises par les Référents.

2. COMMENT LANCER UNE ALERTE

2.1 PROCEDURE D'ALERTE PAR PALIERS

La Loi prévoit deux procédures d'alerte accessibles au lanceur d'alerte : un signalement interne ou un signalement externe.

2.1.1 SIGNALEMENT AU REFERENT INTERNE

En sus des autres canaux de signalement susceptibles d'exister au sein de chaque filiale, le lanceur d'alerte adresse son signalement aux Référents internes désignés par le groupe, joignable à l'adresse email suivante :

compliance@exail-technologies.com

Cette adresse mail n'est consultable que par les Référents de Exail Technologies[5].

Avant de lancer une alerte, chaque Collaborateur pourra – s'il le souhaite – s'adresser à son supérieur hiérarchique ou à toute personne visée dans les points de contact du Code de conduite anti-corruption du groupe ou de sa filiale, ce dernier ayant pour devoir de l'orienter et le conseiller.

2.1.2 SECOND PALIER D'ALERTE : LE SIGNALEMENT EXTERNE

a) A défaut de traitement convenable par l'entreprise de son alerte, le Collaborateur pourra saisir les autorités administratives, judiciaires, un ordre professionnel ou un Défenseur des droits ;
b) A défaut de traitement dans un délai de 3 mois du signalement par l'un des organismes saisis, le signalement pourra être rendu public.
c) En cas de danger grave et imminent ou, pour les informations obtenues dans un cadre professionnel, en cas de danger imminent ou manifeste pour l'intérêt général ou en cas de risque de représailles ou en présence d'un risque de dommages irréversibles (sur la santé, l'environnement, etc), le signalement peut être rendu directement public.

2.2 CONTENU DE L'ALERTE

Afin de pouvoir être traitée, toute alerte doit :

- être rédigée en langue française ou anglaise ;
- comporter l'identité et les coordonnées du lanceur d'alerte ;

Le lanceur d'alerte doit indiquer son identité. Cela évite des dénonciations calomnieuses ou infondées et permet de demander le cas échéant des informations au lanceur d'alerte. Son identité sera protégée par les Référents et le Comité éthique.

Toutefois le lanceur d'alerte peut, s'il le souhaite, rester anonyme lorsque (i) la gravité des faits est établie et (ii) les éléments factuels relatifs à l'alerte sont suffisamment détaillés.

- Indiquer l'identité et les fonctions de la personne faisant objet du signalement ;
- Enoncer les faits signalés ;
- Fournir toutes informations ou documents de nature à étayer son signalement et la gravité des faits signalés.

Le signalement doit être précis et accompagné d'éléments de preuve (courriers, rapports, documents comptables, etc).

[5] Elle pourrait également être accessible aux salariés du service informatique assurant la maintenance du service informatique, en cas de problème informatique des serveurs du groupe.

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

3. COMMENT EST TRAITEE UNE ALERTE

3.1 RECEPTION DE L'ALERTE

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

- adressera au Collaborateur un accusé réception du signalement dans un délai raisonnable
- informera le Collaborateur du délai raisonnable et prévisible dans lequel son signalement sera traité
- indiquera au Collaborateur les modalités suivant lesquelles il sera informé des suites données à son signalement.

3.2 ANALYSE – CONSTITUTION DU COMITE ETHIQUE

A réception d'un signalement, les Référents :

- analysent le caractère sérieux des faits allégués et la recevabilité *prima facie* de l'alerte
- procèdent le cas échéant à des vérifications élémentaires
- Après examen du caractère sérieux des faits invoqués et de la précision des informations données, les Référents forment un Comité éthique, pour décider du traitement de cette alerte, mettre en œuvre une enquête et qualifier les faits.

3.3 ENQUETE INTERNE

- Le Comité éthique liste les actions à prendre et diligente 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 Comité éthique informe les personnes visées par le signalement, sauf en cas de mesure conservatoire pour la collecte de preuves à mettre en œuvre au préalable.
- Le Comité éthique décide de l'opportunité de rédiger un rapport d'enquête ou de faire une restitution verbale de l'enquête.

3.4 RESOLUTION - SUITES DONNEES A L'ALERTE

A l'issue de l'examen de l'alerte par le Comité éthique, quelle que soit l'issue donnée à l'alerte, la décision du Comité éthique sera formalisée dans un document qui sera (en tout ou partie) transmis au lanceur d'alerte par les Référents.

3.5 PRINCIPES FONDAMENTAUX DE TRAITEMENT DE L'ALERTE

Tout signalement sera traité par les Référents et le Comité éthique dans le respect des principes fondamentaux suivants :

- respect de la confidentialité
- protection du lanceur d'alerte
- présomption d'innocence des personnes visées par l'alerte
- respect de la vie privée
- respect du secret médical, le secret lié à la Défense Nationale et le secret professionnel de l'avocat.

3.6 CONSERVATION ET DESTRUCTION DES ELEMENTS DU DOSSIER

Plusieurs hypothèses sont ici à distinguer :

1/ si l'alerte n'entre pas dans le champ d'application du dispositif d'alerte interne, alors la destruction de toutes les données communiquées permettant d'identifier l'auteur du signalement et la personne mise en cause sera réalisée par les Référents sans délai.

2/ Si l'alerte entre dans le champ d'application du dispositif d'alerte interne, alors les Référents procèderont à la destruction de toutes les données communiquées dans les délais suivants :

- Si l'alerte est suivie d'une procédure disciplinaire, ou qu'une procédure judiciaire est engagée : destruction des éléments du dossier de signalement permettant d'identifier l'auteur du signalement et la personne mise en cause, promptement après la clôture de la procédure disciplinaire ou judiciaire engagée ;
- Si aucune suite n'est donnée à l'alerte : destruction des éléments du dossier de signalement permettant d'identifier l'auteur du signalement et la personne mise en cause, dans les 2 mois de la fin de l'analyse de la recevabilité ou des opérations de vérification.

Dans tous les cas, les Référents gardent les éléments anonymisés permettant d'établir le nombre, les motifs des alertes reçues, les suites données. L'ensemble de ces éléments permettront le cas échéant la mise à jour du programme anti-corruption du groupe.

4. PROTECTION DU LANCEUR D'ALERTE

Conformément aux dispositions de la Loi Sapin 2, un lanceur d'alerte qui agit de bonne foi et de manière désintéressée ne peut être écarté d'une procédure de recrutement, de l'accès à un stage ou à une formation professionnelle ; aucun salarié 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.

Evidemment, 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 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.

5. CONFIDENTIALITE ET GESTION DES DONNEES PERSONNELLES

5.1 GESTION DE LA CONFIDENTIALITE

Le respect de la confidentialité étant l'un des principes fondamentaux de traitement d'une alerte, il est rappelé que l'identité du lanceur d'alerte ne sera pas communiquée à la (les) personne(s) mise(s) en cause dans l'alerte, sauf accord du lanceur l'alerte.

Lors du traitement d'une alerte, seules les informations suivantes seront enregistrées :

- L'identité, fonctions et coordonnées du lanceur d'alerte, des personnes faisant l'objet de l'alerte, 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 réception, le traitement et le classement d'une alerte seront traités de manière confidentielle, sous réserve des obligations découlant de la loi ou des procédures judiciaires applicables. Des mécanismes spécifiques ont ainsi été mis en place afin de garantir une stricte confidentialité de : (i) l'identité des lanceurs d'alerte ; (ii) l'identité des personnes visées par l'alerte ; et (iii) des informations recueillies par l'ensemble des destinataires du signalement. Ces mécanismes comprennent notamment la mise en place : (i) d'une adresse mail dont l'accès est restreint aux seuls Référents, (ii) d'un espace de stockage (ou Cloud) hébergé localement et dont l'accès aux serveurs est sécurisé, (iii) d'une charte éthique signée par les membres du Comité éthique (y compris les Référents) les informant des sanctions applicables en cas de violation de la confidentialité ; (iii) d'accords de confidentialité avec tout tiers lorsque la vérification ou le traitement d'une alerte nécessitera une expertise externe ; et (iv) de modalités de destruction ou archivage des données.

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.

5.2 DONNEES A CARACTERE PERSONNEL

Toute donnée à caractère personnel communiquée par un Collaborateur en application du présent dispositif d'alerte interne 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 2, et plus généralement aux obligations légales applicables à Exail Technologies. Elles seront enregistrées dans un fichier informatisé, pourront être transmises au Comité éthique ainsi qu'aux autorités administratives et judiciaires compétentes.

Ces données ne seront conservées que le temps strictement nécessaire et proportionné à leur traitement et à la protection de leurs auteurs.

L'émetteur de l'alerte et la personne faisant l'objet de l'alerte peuvent à tout moment accéder aux données les concernant et en demander, si elles sont inexactes, incomplètes, équivoques ou périmées la rectification ou la suppression. Une telle demande est à formuler auprès des Référents, au moyen de l'adresse email compliance@exail-technologies.com, étant cependant entendu que la personne faisant l'objet d'une alerte ne peut en aucun cas obtenir des informations concernant l'identité du lanceur d'alerte.

6. A RETENIR

↘ Le présent dispositif d'alerte interne est instauré en application de la Loi Sapin 2.

↘ Il vient en sus des procédures le cas échéant applicable au sein de chaque filiale. Il ne constitue pas une obligation mais une option supplémentaire offerte aux Collaborateurs.

↘ Le dispositif définit les modalités de lancement et de traitement d'une alerte par un Collaborateur.

↘ 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.