



CHARTRE DU LANCEUR D'ALERTE



1. CONDITIONS D’UTILISATION DU DISPOSITIF

Le Groupe a mis en place une ligne de lanceur d’alerte externalisée qui permet à ses Collaborateurs de remonter des signalements par l’intermédiaire d’un intervenant externe qui leur donne toutes les garanties en matière de confidentialité et de neutralité. Lorsqu’ils relèvent du champ d’application défini au 2 ci-dessous, les signalements sont transmis au Group Compliance Officer qui est responsable de leur traitement.

Les modes de communication des alertes sont précisés dans l’article 9 de la charte.

Toutefois, ce dispositif n’exclut pas la possibilité de signaler des actes qui pourraient paraître contraires aux lois et règles qui régissent les thèmes énoncés à l’article 2 en passant par la ligne hiérarchique ou en s’adressant à un interlocuteur qualifié pour traiter de cette question : référent Compliance et Compliance Officer, (dont les coordonnées de contact figurent sur le site <https://integrity.eliorgroup.net/>) ou également Directeur juridique et Directeur des Ressources Humaines. Ce signalement se fera par le moyen qui paraîtra le plus adapté au Collaborateur : entretien individuel, courrier, email, appel téléphonique.

Dans tous les cas, la politique du groupe Elior est de favoriser l’expression de ses Collaborateurs et de les protéger de toute conséquence négative, pourvu qu’ils agissent de bonne foi et qu’ils s’appuient sur des éléments vérifiables. Dans cet esprit, les Collaborateurs veilleront à rester, dans leurs signalements, le plus factuel possible et à garder un lien direct avec l’objet de l’alerte.

L’utilisation de bonne foi du dispositif de lanceur d’alerte 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.

En revanche, toute communication effectuée de mauvaise foi, ayant pour but de nuire à des personnes ou à des sociétés, ou qui comporterait des allégations que son auteur sait être fausses pourra faire l’objet de sanctions disciplinaires voire pénales.

2. CHAMP D’APPLICATION

Le dispositif de lanceur d’alerte peut être utilisé pour communiquer des informations relatives aux thèmes suivants :

- Infraction aux règles de concurrence
- Corruption
- Trafic d’influence
- Conflits d’intérêts
- Blanchiment d’argent
- Violation des règles d’embargo international
- Financement du terrorisme
- Fraude
- Inobservation des règles posées par le guide de l’Intégrité du groupe, la charte éthique ou les règles de la concurrence
- Devoir de vigilance (atteintes graves à l’environnement ou envers les droits humains et les libertés fondamentales)

Les signalements peuvent concerner tous les Collaborateurs du Groupe, quel que soit leur niveau hiérarchique et leur statut : dirigeants, salariés, intérimaires, apprentis, stagiaires.

3. PROTECTION DU LANCEUR D’ALERTE

Les lanceurs d’alerte sont protégés, en particulier, par l’application des dispositions des articles 6 à 16 de 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.

Ils bénéficient d’un statut visant à

les protéger de toutes conséquences négatives du fait de l’utilisation de la ligne de lanceur d’alerte.

Pour assurer leur protection sur le plan pratique, ils sont libres de choisir, lorsqu’ils procèdent à un signalement, entre l’une ou l’autre des modalités suivantes :

- soit ils conservent l’anonymat et leur signalement sera examiné dans les mêmes conditions que les autres signalements, si ce n’est qu’il ne sera matériellement pas possible de les tenir informés de la suite donnée à leur signalement. Leur attention est en outre attirée sur le fait que cette absence de dialogue pourra rendre moins efficace l’enquête qui sera diligentée. De plus, leur signalement ne sera pris en compte qu’après un premier examen pour s’assurer que la gravité des faits mentionnés est établie et que les éléments factuels sont suffisamment détaillés.
- soit ils acceptent de révéler leur identité ; dans ce cas le groupe Elior s’engage à mettre en œuvre toutes les mesures nécessaires pour garantir la confidentialité de leur identité. Le lanceur d’alerte pourra être informé des suites données à son signalement et, le cas échéant le Group Compliance Officer pourra prendre contact avec lui de manière confidentielle pour demander des précisions quant au contenu de l’alerte ; les informations recueillies seront traitées avec le même niveau de protection que le signalement initial.

Quel que soit le mode choisi, le dépôt du signalement dans le coffre-fort électronique sera horodaté. Dans le cas d’un signalement non anonyme, un accusé de réception sera envoyé au lanceur d’alerte lui indiquant en particulier la date et l’heure de réception du signalement ainsi qu’une récapitulation des pièces jointes communiquées par lui.

Le groupe Elior met à la disposition de ses collaborateurs (salariés, dirigeants, préposés, etc.)

y compris occasionnels (intérimaires, apprentis, stagiaires, etc.) (ci-après ensemble les « Collaborateurs »)

un dispositif de lanceur d’alerte qui peut être joint :

- Par téléphone en utilisant un des numéros figurant au paragraphe 9 de cette charte
- Par mail à l’adresse alert.eliorgroup@isope.solutions

Avant d’utiliser cette ligne, il est important de lire en entier cette charte qui détaille les modalités de fonctionnement de ce service ainsi que les droits et obligations de chacun.

Il est souligné que le groupe Elior appliquera le principe de proportionnalité dans l’éventuelle application de sanctions en cas d’alerte avérée.

4. CONFIDENTIALITÉ / TRAITEMENT DES DONNÉES COLLECTÉES

Le groupe Elior garantit un traitement confidentiel de toutes les informations qui lui sont transmises par le biais de ce dispositif.

En particulier toutes les données personnelles relatives à l’identité du lanceur d’alerte, les détails du signalement et les preuves éventuellement fournies sont cryptées et conservées dans un coffre-fort électronique hébergé en dehors du groupe auquel seul le Group Compliance Officer peut avoir accès en sa qualité de récipiendaire unique.

L’identité du ou des lanceurs d’alerte n’est communiquée, si cela est nécessaire, au sein de l’entreprise qu’aux seules personnes qui doivent la connaître pour les besoins de la vérification ou du traitement de l’alerte et de ses conséquences et uniquement après qu’elles aient signé un engagement spécifique de confidentialité. L’identité des lanceurs d’alerte n’est en aucun cas communiquée aux personnes concernées par le signalement.

En dehors des cas cités ci-dessus, les éléments de nature à identifier le lanceur d’alerte ne peuvent être divulgués sans le consentement de la personne, sauf à l’autorité judiciaire ou pour satisfaire une exigence légale. De la même manière, les éléments de nature à identifier la personne mise en cause par un signalement ne peuvent être divulgués, sauf à l’autorité judiciaire ou pour satisfaire une exigence légale, qu’une fois établi le caractère fondé de l’alerte.

Les données collectées ne seront conservées que pour la durée nécessaire au traitement du cas examiné. Elles seront détruites dès que leur conservation n’apparaîtra plus nécessaire d’un point de vue légal (en particulier, selon la durée d’une procédure contentieuse) ou,

lorsque cela est techniquement possible, conservées de manière anonyme (c’est-à-dire en neutralisant les données personnelles au sein des données conservées). Pendant la durée de leur conservation, les données personnelles seront stockées sur un système d’information distinct à accès restreint, l’accès au traitement s’effectuant grâce à un identifiant et un mot de passe individuel. Seuls le Group Compliance Officer et le prestataire externe auront la possession de l’identifiant et du mot de passe.

5. DESCRIPTION DES DONNÉES À CARACTÈRE PERSONNEL COMMUNIQUÉES PAR LE LANCEUR D’ALERTE

Le dispositif d’alerte n’enregistre que les données personnelles reçues du lanceur d’alerte ou nécessaires au traitement de l’alerte et qui sont généralement les suivantes :

- Identité, coordonnées et fonction du ou des lanceurs de l’alerte,
- Identité, fonction et coordonnées des personnes faisant l’objet d’une alerte,
- Identité, fonction et coordonnées des personnes intervenant dans le recueil ou le traitement de l’alerte, lorsque cela est nécessaire,
- Faits signalés,
- Éléments recueillis dans le cadre de la vérification des faits signalés,
- Compte-rendu des opérations de vérification, suite donnée à l’alerte.

Les données collectées à l’intérieur de l’Espace Économique Européen ne seront pas transférées dans un pays extérieur à l’Espace Économique Européen.

6. TRAITEMENT DES INFORMATIONS COMMUNIQUÉES

Le recueil des éléments est confié à un prestataire extérieur (iSope Solutions), responsable de la collecte

des données visées à l’article 5 ci-dessus. Il garantit le respect de la confidentialité des données collectées et vérifie que les signalements relèvent du champ d’application défini à l’article 2 et que les informations recueillies présentent une gravité et une cohérence suffisantes pour faire l’objet de vérifications approfondies. Si tel n’est pas le cas, il informe le lanceur d’alerte qu’aucune suite ne sera donnée et l’oriente vers un interlocuteur interne. Un rapport mensuel de ces signalements sans suite sous une forme anonymisée est adressé au Group Compliance Officer, puis toutes les données liées à ces signalements sont détruites.

Dans l’hypothèse où le signalement entre dans le champ d’application défini au point 2 et est suffisamment étayé, il est transmis au Group Compliance Officer qui procède, dans un délai de deux mois, à une vérification des faits évoqués. Au terme de ce délai, une décision est prise sur les suites à donner. Le Group Compliance Officer en informe le lanceur d’alerte.

7. INFORMATION DE LA PERSONNE FAISANT L’OBJET DE L’ALERTE

Conformément notamment à l’article 14 du Règlement Général sur la Protection des Données (« RGD »), le Group Compliance Officer informe la personne visée par une alerte dès l’enregistrement des données la concernant. Il lui indique les faits qui lui sont reprochés, ainsi que les modalités d’exercice de ses droits d’accès et de rectification. Toutefois, l’information de la personne mise en cause peut n’intervenir qu’après l’adoption de mesures conservatoires lorsque celles-ci s’avèrent indispensables, notamment pour prévenir la destruction de preuves nécessaires au traitement de l’alerte.

8. DROIT D’ACCÈS ET DE RECTIFICATION

Conformément aux articles 15 et 16 du RGD, toute personne identifiée dans le dispositif de lanceur d’alerte peut accéder aux données la concernant et en demander, le cas échéant, la rectification ou la suppression. Conformément au RGD, une personne peut également s’opposer au traitement dont elle fait l’objet mais uniquement dans les limites de l’article 21 du RGD (c’est-à-dire que des motifs légitimes et impérieux peuvent prévaloir sur les intérêts et les droits et libertés de la personne concernée). Elle ne peut obtenir communication, sur le fondement de son droit d’accès, des informations concernant des tiers et en particulier l’identité du lanceur d’alerte.

Pour toute information ou exercice de droits en lien avec la protection des données personnelles, le lanceur d’alerte ou toute personne concernée peuvent s’adresser à : gdp-contact@eliorgroup.com

9. INFORMATIONS PRATIQUES

Conformément aux articles 15 et 16 du RGD, toute personne identifiée dans Pour communiquer un signalement, en dehors de la voie hiérarchique ou des interlocuteurs identifiés à l’article 1, trois canaux de communication peuvent être utilisés :

Le courriel à l’adresse : alert.eliorgroup@isope.solutions

Le courrier postal à l’adresse :

iSope solutions (Alerte Elior)
90/92 Route de la Reine
92100 Boulogne-Billancourt - France

Le téléphone pour l’Union Européenne :
Composez le 00 800 180 620 19 du lundi au vendredi de 9h à 18h (CET).
Après avoir sélectionné la langue de votre choix (français, anglais, espagnol, italien ou portugais) un opérateur vous répondra dans la langue que vous aurez choisie.