



Systeme de management intégré

Mode opératoire Transmission et traitement des alertes

Objet du mode opératoire

Le Groupe Idex (“le Groupe”) s’engage à faire preuve d’exigence en matière d’éthique en agissant dans le respect des principes d’intégrité, de transparence et de respect des droits humains en vertu de son **Code de conduite anticorruption** et de sa **Politique d’engagement environnemental, social et sociétal**.

Dans ce cadre, en application de la loi du 9 décembre 2016 *relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique* (dite “loi Sapin II”), de la loi du 27 mars 2017 *relative au devoir de vigilance des sociétés mères et des entreprises donneuses d’ordre* et de la loi du 21 mars 2022 visant à améliorer la protection des lanceurs d’alerte, le Groupe a mis en place un mode opératoire de transmission et de traitement des alertes permettant aux collaborateurs et autres parties prenantes du Groupe :

- de signaler les violations ou manquements graves à l’éthique (“une alerte”) ;
- de poser une question ayant trait à l’éthique (“une question”).

Domaine d’application du mode opératoire

Le lanceur d’alerte

La personne émettant une alerte doit nécessairement satisfaire aux conditions cumulatives suivantes pour que son alerte puisse faire l’objet d’un traitement :

- être une personne physique ;
- être de bonne foi (les déclarations mensongères sont sanctionnables pénalement) ;
- agir de manière désintéressée (sans attendre de contrepartie financière) ;
- ne pas révéler d’informations couvertes par le secret-défense, le secret médical ou le secret professionnel entre un avocat et son client.

Le lanceur d’alerte n’a pas l’obligation d’avoir personnellement connaissance des faits qu’il signale. À ce titre, il peut émettre une alerte en ayant connaissance des faits qui en sont l’objet de manière incidente.

L’objet de l’alerte

Les informations qui peuvent faire l’objet d’une alerte portent sur les violations ou tentatives de violations suivantes :

- un crime ou un délit ;
- une violation grave ou manifeste de la loi ou du règlement ;
- une violation grave ou manifeste d’un engagement international ratifié ou approuvé par la France ou d’un acte d’une organisation internationale ou de l’Union européenne ;
- une menace ou un préjudice grave pour l’intérêt général.

Les faits objets d’une alerte peuvent également concerner des tentatives de dissimulation des violations précitées.

Le dispositif d’alerte concerne tout fait ou situation contraire aux règles et principes édictés par le **Code de conduite anticorruption** et la **Charte éthique** du Groupe (ci-après “violations du code de

conduite anticorruption ou de la charte éthique”) :

- favoritisme, prise illégale d'intérêts, concussion, détournement de fonds publics, trafic d'influence, corruption, conflits d'intérêts ;
- fraude financière ou fiscale, abus de biens sociaux ;
- pratiques anticoncurrentielles ;
- discrimination ;
- harcèlement moral et/ou sexuel ;
- atteintes à l'environnement ;
- atteintes aux droits humains et aux libertés fondamentales (travail forcé, travail dissimulé, exploitation, conditions de travail illégales) ; etc.

1. Un signalement peut d'une part être émis par un collaborateur du Groupe

Les signalements concernant des dysfonctionnements dans la relation de travail avec son manager, son collaborateur ou son équipe, des violations des processus RH internes, des conflits interpersonnels, de mauvaises conditions de travail, des pratiques managériales irrespectueuses (micro-management, manque de reconnaissance, objectifs jugés irréalisables, problématiques de rémunération ou de gestion du temps de travail, mauvaise répartition de la charge de travail, etc.) relèvent de la compétence du référent RH, qui est le canal privilégié pour la réception et le traitement de ces signalements, qui n'ont pas vocation à entrer dans le champ d'application du présent mode opératoire.

Ces situations peuvent toutefois entrer dans le champ d'application du présent mode opératoire si :

- elles persistent car n'ont pas fait l'objet d'un traitement approprié ;
- elles font apparaître des situations de conflits d'intérêts affectant la DRH de proximité ;
- elles présentent des situations d'une particulière gravité, comme le harcèlement moral/sexuel ou la discrimination (ci-après “des dysfonctionnements graves dans la relation de travail”).

Les manquements aux obligations de l'employeur en termes de sécurité, de santé et d'hygiène doivent être signalés via le canal de l'application Ma Sécurité et sortent du champ d'application du présent mode opératoire. Le signalement de ces manquements sera traité en application des procédures du Groupe en matière de santé et de sécurité.

2. Un signalement peut d'autre part être émis par une partie prenante externe du Groupe

Une alerte émise par un tiers via le canal du comité éthique (alertes@idex.fr) est reçue par le comité éthique, qui pourra soit procéder à son instruction, soit transmettre le signalement aux personnes compétentes au sein du Groupe pour le traiter (direction financière, agence ou usine locale, direction santé/sécurité, etc.).

Les cas dans lesquels mobiliser le dispositif d'alerte

Avant de décider de mobiliser le dispositif d'alerte, il peut être utile de se poser les questions suivantes :

- en quoi consiste le manquement constaté ?
- la situation constatée enfreint-elle la loi et/ou les règles internes du Groupe ?
- quand cette situation s'est-elle produite ?
- le Groupe a-t-il déjà remédié à cette situation ?
- de quelle façon cette situation serait-elle considérée par d'autres personnes ?
- quelles conséquences cette situation a-t-elle pour le Groupe ?

Il est parfaitement légitime de s'interroger sur certains comportements et le collaborateur ou la partie prenante qui souhaite déclarer une alerte ou qui s'interroge sur ses propres pratiques est invité, en cas

de doute, à formuler toute remarque ou question. **Un comportement ou une situation anormale ne doit pas être ignoré, même en cas de doute. Il est donc fortement recommandé de ne pas rester isolé et de partager ses questionnements et ses préoccupations en suivant, le cas échéant, la procédure décrite ci-après.**

Définition / Abréviation

Les termes suivants visés par le présent mode opératoire sont définis comme suit :

- **Alerte** : désigne tout signalement transmis de bonne foi et sans contrepartie financière concernant des informations portant sur un crime, un délit, une menace ou un préjudice pour l'intérêt général, une violation ou une tentative de dissimulation d'une violation du droit international ou de l'Union européenne, de la loi ou du règlement, ou une violation des procédures internes du Groupe, selon les modalités prévues par la procédure de transmission et de traitement des alertes du Groupe.
- **Allégation** : désigne toute affirmation réelle ou supposée portée à l'encontre d'un collaborateur ou d'une partie prenante du Groupe concernant la commission d'un crime ou d'un délit, une menace ou un préjudice pour l'intérêt général, une violation ou une tentative de dissimulation d'une violation du droit international ou de l'Union européenne, de la loi ou du règlement, ou une violation des procédures internes du Groupe.
- **Collaborateur** : désigne une personne physique, dirigeant ou membre du personnel, tel qu'un salarié (CDI et CDD), un apprenti, un stagiaire, un collaborateur extérieur et/ou occasionnel (intérimaire, consultant externe ayant une adresse email terminant par @idex.fr) du Groupe, y compris lorsqu'il opère hors des sites du Groupe.
- **Comité éthique** : désigne la formation composée de la directrice juridique et compliance, de la directrice des ressources humaines, du directeur administratif et financier, de la directrice de l'engagement, du chargé d'éthique et de conformité et de la directrice des relations sociales qui est habilitée à recevoir et instruire des alertes.
- **Délégué à la protection des données personnelles (DPO)** : désigne le collaborateur du Groupe chargé d'assurer la protection des données personnelles transmises *via* le dispositif d'alerte professionnelle ou via tout autre moyen de transmission, et des données collectées dans le cadre des enquêtes internes. Le DPO est joignable à l'adresse : dpo@idex.fr.
- **Dispositif d'alerte professionnelle** : désigne les modalités retenues par le Groupe permettant le recueil des signalements transmis par des collaborateurs ou des parties prenantes portant sur un crime, un délit, une menace ou un préjudice pour l'intérêt général, une violation ou une tentative de dissimulation d'une violation du droit international ou de l'Union européenne, de la loi ou du règlement, ou une violation des procédures internes du Groupe.
- **DRH de proximité** : désigne une direction des ressources humaines régionale ou dédiée à une activité spécifique compétente pour recevoir et instruire une alerte lorsqu'un lanceur d'alerte interne relève de son périmètre d'action.
- **Enquête interne** : désigne la phase d'investigation approfondie consécutive à une alerte ou à d'autres faits portés à la connaissance du comité éthique ou d'une DRH de proximité justifiant le déclenchement d'une investigation destinée à vérifier la matérialité des allégations portées à l'encontre d'un collaborateur ou d'une partie prenante du Groupe.
- **Faits portés à la connaissance du comité éthique ou d'une DRH de proximité** : désigne l'ensemble des éléments ou allégations dont les membres du comité éthique ou les membres d'une DRH de proximité sont susceptibles d'avoir connaissance dans le cadre de leurs fonctions et qui pourraient justifier le déclenchement d'une enquête interne (signalements n'ayant pas été transmis via le dispositif d'alerte professionnelle, résultat d'un contrôle ou d'un audit interne ou externe, poursuite engagée à l'encontre du Groupe, requête transmise au Groupe par une autorité étrangère, etc.).
- **Instruction** : désigne la phase durant laquelle la DRH de proximité ou le comité éthique procède au traitement d'une alerte jugée recevable car entrant dans le champ d'application du présent mode opératoire.

- **Lanceur d'alerte** : désigne tout collaborateur personne physique ou partie prenante qui signale ou divulgue, de bonne foi et sans contrepartie financière, des informations portant sur un crime, un délit, une menace ou un préjudice pour l'intérêt général, une violation ou une tentative de dissimulation d'une violation du droit international ou de l'Union européenne, de la loi ou du règlement, ou une violation des procédures internes du Groupe, dont il a eu connaissance.
- **Partie prenante** : désigne une personne physique ou morale ayant une relation d'affaires existante avec le Groupe ou avec laquelle il est envisagé d'établir une relation d'affaires (clients, fournisseurs, intermédiaires commerciaux, actionnaires, partenaires de groupement, joint-ventures, établissements financiers, assureurs, associations, fondations, etc.).
- **Poursuite engagée à l'encontre du Groupe** : désigne tout contentieux initié à l'encontre du Groupe au sujet d'allégations dont l'objet entre dans le champ d'application du dispositif d'alerte professionnelle et justifie le déclenchement d'une enquête interne en parallèle.
- **Requête d'une autorité étrangère** : désigne toute allégation portée à l'encontre d'un collaborateur ou d'une partie prenante du Groupe par une autorité étrangère justifiant la mise en œuvre d'une enquête interne.
- **Suites données à une alerte** : désigne l'ensemble des conclusions auxquelles peut aboutir le traitement d'une alerte. Il peut s'agir d'un classement sans suites ou d'une décision prise si les allégations sont matérialisées ou non, telles qu'appréciées par le comité éthique ou une DRH de proximité.

L'utilisation du dispositif d'alerte est facultative et sa non-utilisation par un collaborateur ne peut en aucun cas lui être reprochée.

Les droits et obligations du lanceur d'alerte

• Les destinataires de l'alerte

Le lanceur d'alerte peut choisir entre l'alerte interne et l'alerte externe à une autorité compétente (administration, autorité publique indépendante telle que le Défenseur des droits - voir liste en Annexe).

La divulgation publique est possible dans certaines situations :

- après avoir effectué une alerte externe, précédée ou non d'une alerte interne, sans qu'aucune mesure appropriée ait été prise en réponse à cette alerte ;
- en cas de danger grave et imminent ou de danger imminent ou manifeste pour l'intérêt général ;
- lorsque la saisine de l'une des autorités compétentes mentionnées en annexe ferait encourir à son auteur un risque de représailles ou qu'elle ne permettrait pas de remédier efficacement à l'objet de la divulgation.

• La protection garantie aux lanceurs d'alerte

Le lanceur d'alerte qui satisfait aux obligations décrites ci-avant ne s'expose à aucune sanction disciplinaire en raison de son alerte, et ce même si les faits énoncés se révèlent par la suite inexacts ou ne donnent lieu à aucune suite.

En particulier, aucun lanceur d'alerte qui formule une alerte ne pourra, s'il a relaté ou témoigné de bonne foi des faits dont il aurait eu connaissance dans l'exercice de ses fonctions et dans des conditions conformes à la présente procédure :

- être suspendu, mis à pied, licencié ou équivalents ;
- être rétrogradé ou se voir refuser une rémunération, promotion, intéressement ou distribution d'actions ;
- être muté vers d'autres fonctions, lieux de travail ou voir son salaire réduit ou ses horaires de travail ;

- être suspendu des dispositifs de formation de l'entreprise ;
- recevoir des évaluations de performance ou des attestations de travail négatives ;
- faire l'objet de mesures disciplinaires imposées ou administrées ;
- faire l'objet de mesures de coercition, intimidation, harcèlement ou ostracisme ;
- faire l'objet de discriminations ou de traitements désavantageux ou injustes ;
- se voir refuser la conversion du contrat de travail temporaire en contrat de travail permanent lorsqu'il pouvait légitimement espérer se voir offrir un emploi permanent ;
- faire l'objet d'un non-renouvellement ou d'une résiliation anticipée de sa période d'essai ;
- subir un préjudice réputationnel ou des pertes financières ;
- être ajouté sur liste noire à l'échelle sectorielle ou d'une branche d'activité professionnelle ;
- voir son contrat le liant avec le Groupe être résilié si le lanceur d'alerte est un partenaire commercial ;
- voir un permis ou une licence annulé ;
- être orienté de façon abusive vers un traitement psychiatrique ou médical ; etc.

La protection garantie aux lanceurs d'alerte est également garantie :

- aux facilitateurs, entendus comme toute personne physique ou morale de droit privé à but non lucratif qui aide un lanceur d'alerte à émettre une alerte ;
- aux personnes physiques en lien avec un lanceur d'alerte qui risquent de faire l'objet de mesures de représailles dans le cadre de leurs activités professionnelles ;
- aux entités juridiques contrôlées par un lanceur d'alerte, pour lesquelles il travaille ou avec lesquelles il est en lien dans un contexte professionnel.

Si un lanceur d'alerte estime avoir subi de telles mesures, il doit en informer immédiatement le comité éthique qui examinera la démarche et prendra, le cas échéant, les mesures nécessaires afin de remédier à cette situation.

Toute personne physique (ou morale) qui agit de manière dilatoire ou abusive contre un lanceur d'alerte en raison des informations signalées ou divulguées peut être condamnée au paiement d'une amende civile de 60 000 €. Cette amende civile peut être prononcée sans préjudice de l'octroi de dommages et intérêts à la victime de la procédure dilatoire ou abusive.

• Les obligations incombant au lanceur d'alerte

Chaque lanceur d'alerte doit avoir conscience, lorsqu'il signale un comportement ou une situation, que les informations fournies ou allégations sont susceptibles de justifier une enquête interne et d'entraîner des décisions affectant d'autres collaborateurs ou parties prenantes.

L'utilisation abusive du dispositif d'alerte expose son auteur à des sanctions disciplinaires et, le cas échéant, à des poursuites judiciaires.

Description du mode opératoire

Comment émettre une alerte interne ?

Une alerte interne peut être émise selon deux canaux :

- le canal du comité éthique via l'adresse email alertes@idex.fr ;
- le canal hiérarchique en s'adressant directement à son manager, à sa direction des ressources humaines de proximité (ci-après "DRH de proximité") ou directement à l'un des membres du comité éthique.

Quel que soit son canal d'émission et pour favoriser sa recevabilité, un lanceur d'alerte doit décrire les faits concernés par l'alerte de manière précise (date, lieu, personnes concernées, etc.), joindre toute pièce utile et communiquer les coordonnées (nom, adresse email ou numéro de téléphone) auxquelles il souhaite être contacté.

Qui sont les destinataires d'une alerte interne ?

1. Si une alerte est émise via le canal du comité éthique :

Un collaborateur ou une partie prenante externe (client, fournisseur, sous-traitant, partenaire commercial, etc.) du Groupe peut adresser une alerte au comité éthique du Groupe composé des personnes mentionnées dans la section "Définition / Abréviation".

Un lanceur d'alerte peut émettre une alerte destinée au comité éthique de façon anonyme, soit via le canal de l'adresse email alertes@idex.fr en utilisant une adresse email de son choix qui ne permet pas son identification, soit par courrier anonymisé en écrivant à : "Comité Éthique du Groupe IDEX, 18-20 quai du Point du Jour, 92100 BOULOGNE-BILLANCOURT". Les lanceurs d'alerte sont toutefois invités à révéler leur identité afin de permettre un traitement efficace de leur alerte par le comité éthique et, le cas échéant, de leur garantir la meilleure protection possible.

2. Si une alerte est émise via le canal hiérarchique :

Le canal hiérarchique pour la remontée d'alertes est exclusivement accessible aux collaborateurs du Groupe et non aux parties prenantes externes. Un collaborateur peut décider d'adresser une alerte à son manager, à sa DRH de proximité ou à un ou plusieurs membres du comité éthique en s'adressant directement à eux par le canal qu'il souhaite (email, appel téléphonique, courrier).

Un manager qui reçoit une alerte entrant dans le champ d'application du présent mode opératoire (tel que décrit *supra*) a l'obligation d'en référer à sa DRH de proximité ou au comité éthique. Le déclarant est notifié de cette remontée d'informations. La DRH de proximité ou le comité éthique prend en charge le traitement du signalement comme s'il ou elle en avait été directement destinataire.

Une DRH de proximité et/ou un ou plusieurs membres du comité éthique peuvent être directement destinataires d'une alerte, soit directement émise par le lanceur d'alerte, soit transmises par le manager de ce dernier. Un membre du comité éthique qui reçoit une alerte non émise via l'adresse email alertes@idex.fr ou par courrier adressé au comité éthique en informe les autres membres du comité éthique.

Un lanceur d'alerte peut émettre une alerte en utilisant le canal hiérarchique anonymement en utilisant une adresse email qui ne permet pas son identification ou par courrier anonymisé.

Quel que soit le canal choisi, les alertes peuvent être effectuées par téléphone ou par tout autre système de messagerie vocale en s'adressant directement à l'un des destinataires susmentionnés, à la demande de l'auteur 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. L'auteur de l'alerte a dans ce cas la possibilité de vérifier, de rectifier et d'approuver la transcription de la conversation ou le procès-verbal par l'apposition de sa signature.

Comment sont traitées les alertes ?

La réception de l'alerte est confirmée par écrit dans un délai de sept jours ouvrés à compter de son émission, de même que sa recevabilité ou son irrecevabilité au regard de la présente procédure :

- une alerte considérée comme irrecevable n'entre pas dans le champ d'application du présent mode opératoire et est instantanément clôturée après notification du lanceur d'alerte ;
- une alerte considérée comme recevable donne lieu à une enquête interne, soit diligentée par la DRH de proximité compétente, soit par le comité éthique.

Il y a deux catégories d'alertes recevables :

- les alertes qui ont vocation à être traitées par la DRH de proximité concernant les dysfonctionnements graves dans la relation de travail ;
- les alertes qui ont vocation à être traitées par le comité éthique concernant les violations du code de conduite anticorruption ou de la charte éthique.

Dans un souci d'efficacité, lorsqu'une alerte est reçue par un destinataire initial (DRH de proximité ou comité éthique) mais que sa nature relève des compétences de l'autre instance, une réorientation est systématiquement proposée au lanceur d'alerte. Aucun transfert des données relatives au signalement ne sera effectué sans le consentement formel, écrit et explicite de son auteur. Un délai de 7 jours ouvrés lui est accordé pour exprimer son choix. En l'absence de réponse dans les délais, son consentement au transfert de données sera considéré comme acquis.

Canal de réception initial	Nature des allégations	Action et gouvernance
Manager	Dysfonctionnements graves dans la relation de travail	Transmission du signalement par le manager à la DRH de proximité
Manager	Violations du code de conduite anticorruption ou de la charte éthique	Transmission du signalement par le manager au comité éthique
DRH de proximité (reçue du lanceur d'alerte ou de son manager)	Dysfonctionnements graves dans la relation de travail	Traitement par la DRH de proximité
DRH de proximité (reçue du lanceur d'alerte ou de son manager)	Violations du code de conduite anticorruption ou de la charte éthique	Transmission du signalement par la DRH de proximité au comité éthique (si accord du lanceur d'alerte)
Comité éthique (reçue du lanceur d'alerte ou de son manager)	Dysfonctionnements graves dans la relation de travail	Transmission du signalement par le comité éthique à la DRH de proximité (si accord du lanceur d'alerte)
Comité éthique (reçue du lanceur d'alerte ou de son manager)	Violations du code de conduite anticorruption ou de la charte éthique	Traitement par le comité éthique

Si le lanceur d'alerte refuse le transfert de son dossier, il est informé que son alerte est clôturée et est invité à la transmettre lui-même à l'instance pertinente.

Il est formellement interdit à tout membre du personnel non-habilité d'avoir connaissance des informations recueillies dans le cadre d'une alerte.

Quelles suites à une alerte ?

Le lanceur d'alerte est informé dans un délai raisonnable n'excédant pas trois mois à compter de l'accusé de réception de l'alerte ou, à défaut d'accusé de réception, trois mois à compter de l'expiration d'une période de sept jours ouvrés suivant l'émission de l'alerte, des mesures envisagées ou prises pour évaluer l'exactitude des allégations et, le cas échéant, remédier à l'objet de l'alerte.

A réception de l'alerte, si elle est recevable, la DRH de proximité ou le comité éthique instruit l'enquête interne afférente :

- les enquêtes internes instruites par la DRH de proximité mobilisent les collaborateurs de son choix qui lui sont rattachés et la direction des relations sociales est systématiquement notifiée du lancement d'une enquête interne par la DRH de proximité ;
- les enquêtes internes instruites par le comité éthique sont organisées selon les modalités décrites dans la note sur les rôles et responsabilités du comité éthique.

Les enquêtes internes diligentées sur le périmètre du Groupe sont conduites en application du Mode opératoire Enquête interne, qui décrit notamment les moyens d'enquête et le formalisme attendu.

Au terme d'une enquête interne instruite par la DRH de proximité, celle-ci informe le lanceur d'alerte des conclusions de l'enquête et lui indique si les allégations contenues dans son signalement sont matérialisées ou non. Elle formule des recommandations sur les suites à apporter à la hiérarchie du lanceur d'alerte et des personnes mises en cause, ainsi qu'au directeur de l'activité ou directeur régional concerné. La DRH de proximité transmet une synthèse de l'enquête interne au comité éthique pour information et suivi.

Au terme d'une enquête interne par le comité éthique, celui-ci formalise une synthèse d'enquête interne qui formule des recommandations sur les suites à y apporter. Cette synthèse est communiquée au président et au directeur général délégué, qui approuvent formellement cette synthèse et peuvent formuler des remarques. Le synthèse de l'enquête interne signée est transmise à la hiérarchie du lanceur d'alerte et des personnes mises en cause.

En tout état de cause, le lanceur d'alerte est informé sans délai de la clôture de son alerte par écrit, soit lorsque l'alerte est déclarée irrecevable, soit lorsque l'alerte est déclarée recevable et arrive au terme de son traitement par la DRH de proximité ou le comité éthique. Lorsqu'une alerte est jugée recevable, les personnes visées par celle-ci sont également informées sans délai de sa clôture lorsque l'alerte arrive au terme de son traitement.

Si l'alerte a été déposée de manière anonyme et par un autre biais que l'envoi d'un courriel à partir d'une adresse email qui permet d'identifier avec certitude l'identité du lanceur d'alerte, alors il revient à son auteur de se manifester auprès de la DRH de proximité ou du comité éthique pour être informé des suites apportées.

Le Groupe garantit la destruction de toute information permettant l'identification du lanceur d'alerte, des faits objets de l'alerte et des personnes visées par l'alerte sans délai lorsque l'alerte est jugée irrecevable et dans un délai maximum de deux mois lorsque l'alerte est considérée comme recevable mais est classée sans suites, en en informe les personnes concernées.

La gestion des conflits d'intérêts dans le cadre du dispositif d'alerte

Les membres du comité éthique et les DRH de proximité sont soumis à des obligations strictes d'intégrité et de confidentialité concernant l'identité du lanceur d'alerte, les faits objets de l'alerte et les personnes visées par l'alerte.

En cas de conflit d'intérêts entre leur position au sein du Groupe et les faits objets de l'alerte, les membres du comité éthique doivent se départir de tout processus d'analyse ou de traitement en lien avec l'alerte concernée.

En cas de conflit d'intérêts affectant un gestionnaire au sein de la DRH de proximité, celui-ci doit obligatoirement se dessaisir du traitement de l'alerte. Le traitement du signalement sera alors immédiatement attribué à un autre gestionnaire au sein de la DRH ou à des membres du comité éthique impartiaux afin de garantir l'objectivité du traitement de l'alerte.

Les modalités et droits entourant le traitement des données à caractère personnel collectées au travers des alertes

La direction juridique et compliance tient à jour un registre de suivi des alertes reçues par le comité éthique, qu'elle complète avec un reporting trimestriel transmis par chaque DRH de proximité. Le registre mentionne, pour chaque alerte :

- la date de réception ;
- le canal de transmission de l'alerte ;
- le caractère recevable ou irrecevable ;
- la thématique du signalement et sa description ;
- la date de l'accusé-réception transmis au lanceur d'alerte ;
- l'identité des personnes en charge du traitement du signalement ;
- la description des modalités de traitement ;
- le statut du signalement (en cours de traitement, clôturé ou anonymisé) ;
- une description des échanges avec le lanceur d'alerte ;
- la date d'information du lanceur d'alerte sur le statut de son signalement ;
- la date et les modalités d'information des personnes mises en cause ;
- le caractère matérialisé ou non des allégations à l'issue du traitement ;
- la liste des mesures prises à l'issue du traitement ;
- la date d'information du lanceur d'alerte concernant la clôture du signalement.

Les modalités d'application de la présente procédure ont été définies de manière à garantir la conformité à la réglementation applicable en matière de protection des données personnelles, comprenant notamment :

- la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;
- la délibération n° 2023-064 du 6 juillet 2023 portant abrogation de la délibération n° 2019-139 du 18 juillet 2019 portant adoption d'un référentiel relatif aux traitements de données à caractère personnel destinés à la mise en oeuvre d'un dispositif d'alertes professionnelles et adoption d'un référentiel relatif aux traitements de données à caractère personnel destinés à la mise en oeuvre d'un dispositif d'alertes professionnelles ;
- le règlement (UE) 2016/679 du Parlement européen 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

Les DRH de proximité et le comité éthique destinataires des alertes et questions posées les instruisent dans les conditions de confidentialité qui répondent à une exigence stricte et proportionnée au regard de la finalité du traitement.

Dans la limite des seuls besoins de vérification ou de traitement de l'alerte ou de la question posée, et dans la limite des seules informations strictement nécessaires à la finalité poursuivie, les données personnelles traitées dans le cadre du dispositif d'alerte, notamment les données relatives à l'identité et les coordonnées de la personne concernée, pourront également être communiquées :

- à des personnes internes ou externes au Groupe (membres du comité éthique et des DRH de proximité, supports internes mobilisés dans le cadre du traitement des alertes et experts tels que des avocats et autres conseillers professionnels pour la consultation, la défense ou l'exercice des droits en justice), dont le concours est rendu nécessaire dans le cadre du traitement de l'alerte, en raison de leurs missions ou de leurs fonctions ;
- aux autorités compétentes (autorités judiciaires / administratives et organismes de réglementation), conformément aux lois applicables.

Les données à caractère personnel collectées dans le cadre du traitement des alertes sont conservées jusqu'à la détermination des suites à y donner, puis sont anonymisées, sauf dans les cas où des procédures judiciaires ou contentieuses sont engagées, auxquels cas ces données sont conservées jusqu'au terme des procédures avant anonymisation. Les données anonymisées sont conservées sans limitation de durée.

Toute personne identifiée, par quelque moyen que ce soit, dans le cadre du dépôt d'une alerte ou lors de la réalisation d'une enquête interne, a le droit d'accéder aux informations la concernant ainsi que de faire rectifier ou supprimer des informations qu'elle jugerait incomplètes, inexactes, ambiguës ou obsolètes. La ou les personnes mises en cause dans le cadre d'une alerte sont ainsi informées de l'enregistrement de données à caractère personnel la concernant afin de lui permettre de s'y opposer pour un motif légitime et/ou de faire modifier ou supprimer toute information qu'elle estime erronée. Le délégué à la protection des données personnelles est joignable à l'adresse : dpo@idex.fr. Aucun transfert n'est réalisé en dehors de l'Union Européenne ou de l'Espace Economique Européen.

Documents associés

1. Mode opératoire Enquête interne

2. Note sur les rôles et responsabilités du comité éthique

Historique des modifications

Le présent mode opératoire a vocation à être mis à jour ponctuellement, soit lorsque l'entrée en vigueur d'une nouvelle politique ou procédure de conformité au du Groupe modifie ses dispositions, soit lorsque le Comité de direction décide de la modifier.

Objet	Approbation				Date
	Nom	Prénom	Fonction	Signature	
Création	FREMAUX	Benjamin	Président	Oui	10/02/2025
	LE BEUX	Thomas	Directeur général délégué	Oui	
	BONHOMME	Odile	DRH	Oui	
	NICOLAS	Jean-Baptiste	DAF	Oui	
	LECA	Charlotte	Directrice de l'Engagement	Oui	
	CRESSOL	Elodie	Directrice Juridique	Oui	
Mise à jour	FREMAUX	Benjamin	Président	Oui	26/06/2026
	LE BEUX	Thomas	Directeur général délégué	Oui	
	BONHOMME	Odile	DRH	Oui	
	NICOLAS	Jean-Baptiste	DAF	Oui	
	LECA	Charlotte	Directrice de l'Engagement	Oui	
	CRESSOL	Elodie	Directrice Juridique	Oui	

Liste des organismes pouvant être saisis

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 ;

Protection de l'environnement :

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

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) ;

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

Relations individuelles et collectives du travail, conditions de travail :

- Direction générale du travail (DGT) ;

Emploi et formation professionnelle :

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

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 ;

Discrimination :

- Défenseur des droits.