# PROCÉDURE D'ALERTE ET D'ÉCOUTE CONFIDENTIELLE

Ailancy Groupe

Version 05 / 2026

| Élément | Contenu |
| --- | --- |
| Propriétaire | Comité RSE |
| Instance de validation | Comité RSE |
| Périmètre | Groupe Ailancy |
| Version | V1.0 – 2026 |
| Date d’entrée en vigueur | 01/05/2026 |

# Table des matières


**1. Objet et périmètre** ..... 5

**2. Gouvernance et référents** ..... 5

**2.1. Pilotage et responsabilités générales** ..... 5

**2.2. Référents sociaux répartis par entité** ..... 6

**2.3. Référents par thème, indépendamment du rattachement à une entité** ..... 6

**2.4. Orientation simplifiée pour les signalements externes** ..... 7

**2.5. Conflits d'intérêts et suppléance** ..... 7

**3. Deux voies : alerte formelle et écoute / orientation** ..... 8

**3.1. Alerte formelle – « J'alerte »** ..... 8

**3.2. Écoute / orientation confidentielle** ..... 8

**4. Situations pouvant être signalées** ..... 9

**4.1. Catégories de l'alerte formelle** ..... 9

**4.2. Orientation par entité** ..... 10

**5. Canaux de signalement, identité et anonymat** ..... 10

**5.1. Accès interne** ..... 10

**5.2. Accès pour les parties prenantes externes** ..... 10

**5.3. Choix de l'identité et du moyen de contact** ..... 10

**5.4. Signalements de bonne foi et prévention des abus** ..... 11

**6. Dépôt, réception et orientation du signalement** ..... 11

**6.1. Données recueillies dans les formulaires internes** ..... 11

**6.2. Données recueillies par le formulaire externe simplifié** ..... 12

**6.3. Réception sécurisée et attribution** ..... 12

**6.4. Confirmation du dépôt** ..... 12

**7. Analyse et traitement** ..... 13

**7.1. Accusé de réception et délais** ..... 13

**7.2. Première analyse** ..... 13

**7.3. Vérifications et instruction** ..... 13

**7.4. Information pendant l'instruction** ..... 14

**8. Protection des personnes et mesures temporaires** ..... 14

**9. Mesures correctives et clôture** ..... 15

**10. Registre, suivi et reporting** ..... 15
**11. Protection des données, confidentialité et sécurité** ..... 16
**11.1. Confidentialité et habilitations** ..... 16
**11.2. Séparation des rôles et sécurité technique** ..... 16
**11.3. Information, minimisation et traductions** ..... 17
**11.4. Conservation et suppression** ..... 17
**12. Signalements auprès d'autorités externes** ..... 17
**13. Communication, sensibilisation et révision** ..... 18

## 1. Objet et périmètre

Le Groupe Ailancy met à disposition un dispositif d'alerte et d'écoute confidentielle (« Alerte & écoute ») destiné à faciliter le signalement de faits préoccupants, le traitement des manquements et l'orientation des personnes qui souhaitent obtenir une écoute ou un accompagnement.

La présente procédure définit le périmètre du dispositif, ses deux parcours, les canaux accessibles aux personnes internes et externes, l'organisation des référents, les modalités de réception et de traitement des signalements, les garanties de confidentialité et de protection, ainsi que les règles de suivi, de clôture et de conservation des données.

Elle s'applique aux entités du Groupe Ailancy, sous réserve des dispositions impératives du droit local applicables à chaque entité. Le dispositif est accessible aux collaborateurs, salariés, alternants, stagiaires et autres personnes disposant d'un accès approprié, ainsi qu'aux anciens salariés, candidats, fournisseurs, sous-traitants, prestataires, clients, partenaires et autres parties prenantes concernées, selon leur lien avec les faits signalés. L'accès au dispositif ne préjuge pas, à lui seul, de la reconnaissance du statut légal de lanceur d'alerte, appréciée au regard des conditions applicables.

Le dispositif repose notamment sur la loi n° 2016-1691 du 9 décembre 2016 (« Sapin II »), modifiée par la loi n° 2022-401 du 21 mars 2022 (« Waserman »), le décret n° 2022-1284 du 3 octobre 2022, les dispositions pertinentes du Code du travail, le RGPD et le référentiel de la CNIL relatif aux alertes professionnelles (2023). Il s'inscrit également dans les principes de confiance, d'impartialité et de protection de l'ISO 37002:2021, ainsi que dans les politiques d'éthique et de conduite du Groupe.

Les protections prévues pour les lanceurs d'alerte s'appliquent lorsque les conditions légales sont remplies. Toute personne utilisant le dispositif de bonne foi bénéficie, par ailleurs, des garanties internes de confidentialité, d'examen impartial et de non-représailles prévues par cette procédure, sans préjudice des régimes juridiques spécifiques applicables.

## 2. Gouvernance et référents

### 2.1. Pilotage et responsabilités générales

Le Comité RSE est propriétaire de la présente procédure, supervise son fonctionnement sur la base d'informations agrégées et valide ses évolutions significatives. L'équipe RSE assure la coordination opérationnelle du dispositif et la cohérence des deux parcours. Les personnes habilitées à traiter le contenu d'un dossier sont déterminées au cas par cas en fonction de la catégorie, de la compétence requise et de l'absence de conflit d'intérêts.

La Cheffe de projet RSE assure le suivi transversal des éléments de pilotage nécessaires (numéro, dates, catégorie, urgence, référent attribué, statut, échéances

et mesures suivies). Lorsqu'elle n'est pas expressément habilitée à intervenir sur un dossier, cette mission ne lui donne pas accès au récit détaillé, aux identités, aux pièces jointes ni aux échanges confidentiels. La supervision du Comité RSE ne confère pas non plus un accès général au contenu des dossiers.

Les référents désignés disposent, pour les missions qui leur sont confiées, de la compétence, des moyens et de la latitude nécessaires à un traitement impartial. Ils sont tenus à une obligation de confidentialité et à une règle d'accès limité au strict besoin d'en connaître.

### 2.2. Référents sociaux répartis par entité

Pour les questions de harcèlement et comportements sexistes, de RQTH / handicap, de conditions de travail et réclamations ainsi que de QVT / stress / mal-être, l'interlocuteur social est présenté en fonction de l'entité concernée. La voie QVT / stress / mal-être relève uniquement du parcours « Écoute / orientation », sauf si les faits révèlent par ailleurs un manquement ou un risque relevant d'une alerte formelle.

| Entité | Référent(s) social(aux) – écoute / orientation | Référent(s) – alerte formelle si faits relevant d'une alerte |
|---|---|---|
| Ailancy Advisory | Hélène Sellam ; Imane Kassou | Hélène Sellam ; Imane Kassou |
| Ailancy Technology | Yassine Bentama | Yassine Bentama |
| AYGROUP | Davy Bragança | Davy Bragança |
| Ailancy AI & Cyber | Marie-Paule Camara | Marie-Paule Camara |

Lorsqu'une même entité dispose de plusieurs référents, l'attribution du dossier est effectuée à une personne habilitée, après vérification de la compétence et des conflits d'intérêts : la présence de deux noms ne signifie pas un accès simultané et systématique au dossier. Les demandes ordinaires de RQTH relèvent de l'écoute / orientation ; un fait de discrimination, de harcèlement ou un manquement lié au handicap peut relever de l'alerte formelle.

### 2.3. Référents par thème, indépendamment du rattachement à une entité

| Sujet | Écoute / orientation | Alerte formelle / fonction de traitement |
|---|---|---|
| Discrimination / égalité de traitement | Hélène Sellam ou Marie-Paule Camara (RH) | Hélène Sellam ou Marie-Paule Camara (RH) |
| Santé / sécurité / RPS graves | Marie-Paule Camara / Chloé (RH) | Marie-Paule Camara / Chloé (RH) |
| Corruption / fraude / conflits d'intérêts / intégrité | Jacqueline ( Responsable RSE) | Jacqueline (Responsable RSE) |
| Représailles / risque de représailles | Jacqueline (Responsable RSE) | Jacqueline (Responsable RSE) |

| Sujet | Écoute / orientation | Alerte formelle / fonction de traitement |
|---|---|---|
| Droits humains / travail forcé / travail des enfants | Marie-Paule Camara (RH) | Marie-Paule Camara (RH) |
| Données / confidentialité / cybersécurité | Ibrahim (CIO / CDO) | Ibrahim (CIO / CDO) |
| Environnement | Qi Zhang (Cheffe de projet RSE) | Qi Zhang (Cheffe de projet RSE) |
| Autre situation grave / catégorie incertaine | Qi Zhang (Cheffe de projet RSE) | Qi Zhang (Cheffe de projet RSE) première orientation, puis référent compétent |
| Identifier le bon interlocuteur ; passage de l'écoute à l'alerte | Qi Zhang (Cheffe de projet RSE) | Référent compétent selon les faits |

Les référents mentionnés dans ces tableaux constituent des interlocuteurs de compétence et non une liste de destinataires automatiquement autorisés. Lorsque plusieurs personnes sont indiquées, une seule attribution initiale est effectuée, ou une intervention partagée strictement justifiée et documentée.

### 2.4. Orientation simplifiée pour les signalements externes

Les signalements adressés par les canaux accessibles aux parties prenantes externes suivent une répartition simplifiée : (i) les faits relevant de la protection des données, de la confidentialité, des systèmes d'information ou de la cybersécurité sont orientés vers Ibrahim, CIO / CDO ; (ii) les autres faits, y compris les catégories incertaines, sont orientés vers une personne habilitée de l'équipe RSE. Une personne compétente d'un autre service peut être associée par la suite lorsque l'analyse du dossier le justifie, sans donner accès au dossier à l'ensemble des référents internes.

Cette simplification de l'entrée externe n'écarte ni les compétences spécialisées nécessaires au traitement des faits ni les garanties de protection des personnes. Le canal de première réception doit permettre un tri sécurisé avant toute communication du dossier à son référent de traitement.

### 2.5. Conflits d'intérêts et suppléance

Toute personne visée par le signalement, directement impliquée dans les faits ou en situation susceptible d'altérer son impartialité est exclue de la réception du contenu, de l'analyse, de l'instruction et de la décision concernant le dossier. Une demande d'exclusion formulée par l'auteur est examinée avant l'ouverture des droits d'accès au destinataire normalement prévu ; elle ne constitue pas une faculté de désigner librement tout salarié comme enquêteur.

Lorsque le référent normalement compétent est concerné ou empêché, une personne habilitée, indépendante et dotée des compétences nécessaires est désignée. Pour une situation impliquant un membre de la Direction ou un associé, l'orientation

privilégiée est assurée par Jacqueline, Responsable RSE, sous réserve de son indépendance effective. Si Jacqueline ou des membres de l'équipe RSE sont eux-mêmes concernés, une autre personne indépendante est désignée par l'instance compétente, hors de toute personne impliquée ; l'appui d'un conseil externe peut être retenu si nécessaire. Aucune personne mise en cause ne valide sa propre suppléance ni ne consulte le dossier avant réattribution.

Les droits d'accès sont accordés nominativement et révoqués dès qu'ils cessent d'être nécessaires. La séparation entre administration technique et traitement du fond est appliquée, y compris lorsque le CIO / CDO est par ailleurs référent d'une catégorie de signalements.

## 3. Deux voies : alerte formelle et écoute / orientation

L'espace « Alerte & écoute » propose deux parcours clairement distincts. Sur l'Intranet, l'accès se fait depuis la page de présentation du dispositif, puis par les choix « J'alerte » et « Je souhaite être écouté(e) / orienté(e) ». Chaque parcours indique les garanties de confidentialité et le référent ou la fonction susceptible d'intervenir.

### 3.1. Alerte formelle – « J'alerte »

Cette voie permet de signaler des faits susceptibles de constituer une violation de la loi ou des règles applicables, un manquement à l'éthique du Groupe, une discrimination, un harcèlement, une atteinte aux droits humains, un incident grave ou toute autre situation justifiant un traitement formalisé. Elle donne lieu à un enregistrement, une première qualification, des vérifications adaptées, un retour dans les délais applicables et une clôture documentée.

Avant de déposer l'alerte, l'auteur accède à une page d'information présentant notamment la protection de bonne foi, l'interdiction des représailles, les règles de confidentialité, les choix relatifs à l'identité, les éventuelles limites techniques de l'anonymat, le processus et les voies de signalement auprès des autorités compétentes. Il peut ensuite poursuivre vers le formulaire.

### 3.2. Écoute / orientation confidentielle

Cette voie permet de demander une écoute, un accompagnement ou l'identification du bon interlocuteur sans ouvrir automatiquement une enquête formelle. Elle s'adresse notamment aux personnes confrontées à une difficulté de QVT, un stress, un mal-être, une question de RQTH / handicap, une difficulté relative aux conditions de travail ou un doute sur la nature d'une situation vécue ou observée.

Le formulaire d'écoute suit une présentation cohérente avec le parcours d'alerte : besoin exprimé, entité lorsque pertinente, possibilité de ne pas renseigner l'identité, message libre, interlocuteur pressenti et éventuelle objection liée à un conflit d'intérêts. Il n'applique pas automatiquement les qualifications ni les mêmes exigences de traitement qu'une alerte relevant de la loi Sapin II.

Si les échanges font apparaître des faits qui justifient une alerte formelle, la personne est orientée vers le parcours adapté, sans présumer de son consentement à l'ouverture d'une enquête. Cette absence d'automaticité ne fait pas obstacle aux mesures que le Groupe doit prendre pour respecter ses obligations de santé, de sécurité ou de protection des personnes. Tout transfert d'informations se limite à ce qui est nécessaire et légalement permis.

## 4. Situations pouvant être signalées

Le choix de catégorie sert à orienter l'examen ; il ne constitue pas une qualification juridique définitive. Une même situation peut correspondre à plusieurs rubriques. L'auteur sélectionne la plus proche et décrit librement les autres aspects utiles.

### 4.1. Catégories de l'alerte formelle

- Éthique des affaires / intégrité : corruption, fraude, conflits d'intérêts, cadeaux ou invitations inappropriés, irrégularités commerciales, non-respect du Code de conduite.
- Harcèlement / comportements sexistes : harcèlement sexuel, agissements sexistes, harcèlement moral, humiliations répétées, isolement, pressions abusives et comportements susceptibles de dégrader les conditions de travail.
- Discrimination / égalité de traitement : traitement défavorable lié notamment à l'origine, au sexe, à l'âge, au handicap, à l'état de santé, à la religion, à l'orientation sexuelle, aux opinions ou aux activités syndicales, ainsi qu'à tout autre critère protégé.
- Conditions de travail / réclamations nécessitant un traitement formalisé : difficulté suffisamment caractérisée concernant l'organisation, la charge ou les conditions de mission et appelant un examen documenté ; l'existence d'une réclamation ne signifie pas nécessairement qu'elle relève du statut légal de lanceur d'alerte.
- Droits humains / travail forcé / travail des enfants : faits potentiellement liés aux activités du Groupe ou à ses relations avec un fournisseur, sous-traitant, prestataire ou partenaire.
- Protection des données / confidentialité / cybersécurité : fuite de données, accès non autorisé, usage inapproprié d'informations sensibles, incident de confidentialité ou de sécurité.
- Représailles ou risque de représailles : toute mesure défavorable liée à un signalement, une demande de soutien, un témoignage ou la participation à une vérification.
- Santé / sécurité / RPS graves : risque grave ou imminent pour la santé physique, psychologique ou la sécurité.
- Environnement : risque environnemental grave, manquement important à une obligation applicable ou situation susceptible d'avoir un impact environnemental significatif.

- Autre situation grave / catégorie incertaine : faits dont l'auteur ne sait pas déterminer le domaine ou qui ne correspondent à aucune rubrique précédente.

Les demandes ordinaires relatives à la RQTH et les situations générales de QVT / stress / mal-être sont orientées vers le parcours « Écoute / orientation ». En revanche, une discrimination liée au handicap, un refus susceptible de constituer un manquement, un harcèlement ou un risque grave peut être signalé par la voie formelle.

### 4.2. Orientation par entité

Pour les sujets sociaux indiqués au § 2.2, le rattachement à l'entité concernée est pris en compte afin d'afficher l'interlocuteur pertinent. L'absence de certitude sur l'entité ne bloque pas le dépôt : l'auteur peut choisir « Je ne sais pas », et l'attribution est déterminée à partir des faits disponibles.

## 5. Canaux de signalement, identité et anonymat

### 5.1. Accès interne

Les personnes disposant des droits nécessaires utilisent l'espace permanent « Alerte & écoute » de l'Intranet. Celui-ci propose les deux voies décrites au § 3. Les formulaires affichent clairement l'identité ou la fonction du référent normalement prévu, tout en permettant de signaler un conflit d'intérêts avant tout accès de ce dernier au dossier.

### 5.2. Accès pour les parties prenantes externes

Les personnes sans accès Intranet disposent de deux moyens de transmission : l'adresse électronique dédiée alerte@ailancy.com et un formulaire confidentiel présenté sur le site Internet du Groupe après validation et mise en service de ses fonctions de sécurité. La page publique présente ces deux choix à égalité, sans obliger le déclarant à connaître les référents internes.

Le canal proposé sur le site Internet du Groupe constitue un canal de signalement auprès d'Ailancy (signalement interne au sens de la réglementation), et non une saisine d'une autorité externe indépendante. L'accès par e-mail reste possible indépendamment de la disponibilité technique du formulaire.

La page publique indique de façon concise qui peut signaler, les grands types de faits, les garanties de confidentialité, le choix relatif à l'identité, les délais de retour et le lien vers les informations relatives aux données personnelles. Elle précise également que le déclarant peut saisir directement les autorités compétentes selon les règles applicables.

### 5.3. Choix de l'identité et du moyen de contact

Le déclarant peut : (i) renseigner son identité et un moyen de contact ; (ii) ne pas renseigner son identité mais fournir un moyen de contact non nominatif ; ou (iii) ne fournir ni identité ni moyen de contact, lorsque le canal le permet. Le choix est présenté avant les autres questions afin de ne pas dissuader inutilement un signalement.

L’absence d’identité n’est pas, à elle seule, un motif d’exclusion. Les signalements anonymes sont examinés en fonction des faits communiqués et des possibilités de vérification. En revanche, l’absence de moyen de contact peut empêcher l’envoi d’un accusé personnalisé, les demandes de précision ou le retour d’information. Lorsque la plateforme permet un espace d’échange sécurisé associé à un numéro de dossier, les échanges peuvent s’y poursuivre sans imposer la divulgation du nom.

Le courriel peut révéler l’adresse de son expéditeur : la voie e-mail est confidentielle, mais elle n’offre pas à elle seule la garantie d’une absence d’identification. De même, un formulaire Web ou Intranet peut générer des données techniques de connexion ; celles-ci sont strictement limitées et protégées et ne doivent pas servir à rechercher systématiquement l’identité des personnes qui ont choisi de ne pas la communiquer. Aucune garantie d’anonymat absolu n’est annoncée sans vérification technique correspondante.

### 5.4. Signalements de bonne foi et prévention des abus

Les signalements sont effectués de bonne foi, sans obligation pour leur auteur de fournir une démonstration juridique ou des pièces probantes complètes. Un signalement non confirmé, inexact ou insuffisamment étayé n’établit pas, en soi, une mauvaise foi. Seules les situations de mensonge intentionnel ou d’usage manifestement malveillant, établies sur la base d’éléments objectifs, peuvent donner lieu aux mesures prévues par les règles applicables. Aucun justificatif d’identité n’est exigé de manière systématique à l’entrée du dispositif.

## 6. Dépôt, réception et orientation du signalement

### 6.1. Données recueillies dans les formulaires internes

Pour l’alerte formelle, le formulaire recueille les seuls éléments nécessaires à une première analyse : choix relatif à l’identité et au contact, lien avec les faits, catégorie principale, description libre, éventuelles personnes ou entités concernées, urgence, besoin de protection, pièces jointes facultatives, référent initialement affiché et éventuel conflit d’intérêts. Les champs de poste, manager ou projet ne sont pas systématiquement exigés et restent facultatifs lorsque leur précision n’est pas nécessaire.

L’auteur décrit les faits dans la langue dans laquelle il s’exprime le plus clairement, sans devoir utiliser de termes juridiques. Toute traduction nécessaire est organisée par une personne ou un prestataire habilité, soumis à des garanties de confidentialité et de protection des données.

Une validation finale rappelle l’exigence de bonne foi, le caractère confidentiel du traitement et l’existence des informations relatives au fonctionnement du dispositif et à la protection des données. L’enregistrement produit un numéro de dossier qui permet de retrouver la référence du signalement.

### 6.2. Données recueillies par le formulaire externe simplifié

Le formulaire public privilégie un nombre limité de questions : nature du signalement (données / informatique / cybersécurité ; autre situation ; catégorie incertaine), lien éventuel avec le Groupe, choix d'identité et de contact, description libre des faits, pièces jointes facultatives et possibilité d'indiquer un conflit d'intérêts. Si cela est utile et connu, l'auteur peut préciser l'entité ou le pays concerné ; leur identification n'est pas un préalable obligatoire au dépôt.

Le formulaire ne demande ni la connaissance des référents du Groupe ni une identification nominative obligatoire. La possibilité de signaler l'implication d'un destinataire normalement prévu est maintenue, afin que la réattribution puisse intervenir avant consultation du dossier par une personne concernée.

### 6.3. Réception sécurisée et attribution

Chaque signalement est enregistré dans un espace ou circuit de réception sécurisé avec une date de réception et une référence unique. Les accès aux pièces et aux échanges sont réservés aux personnes expressément habilitées. Les courriels reçus sur l'adresse dédiée ne sont pas redirigés vers une boîte aux lettres partagée ordinaire ni diffusés à une liste de collaborateurs. Le personnel assurant le tri initial est tenu au secret et ne peut conserver plus d'informations que celles nécessaires à l'orientation.

La catégorie et, pour les sujets sociaux internes, l'entité servent à proposer le référent compétent. L'attribution finale n'est réalisée qu'après examen de l'urgence et d'éventuels conflits d'intérêts. L'équipe RSE ne dispose pas, du seul fait de sa mission de pilotage, d'un accès généralisé aux dossiers dont elle n'assure pas la réception ou le traitement. Les signalements externes sont orientés suivant la règle simplifiée du § 2.4.

Les personnes expressément écartées en raison d'un conflit d'intérêts ne reçoivent ni notification contenant des faits sensibles ni droit d'accès au dossier. Une réattribution, son motif général et les droits effectivement ouverts sont consignés de manière sécurisée.

### 6.4. Confirmation du dépôt

Lorsque le canal le permet, la page de confirmation indique que le signalement a été transmis, affiche le numéro de dossier et décrit les grandes étapes du traitement. Elle rappelle les délais de réception et de retour d'information, sans les confondre avec un délai maximal de clôture de l'enquête. Si le dépôt s'effectue par e-mail, l'accusé de réception est envoyé par le canal sécurisé approprié lorsque l'auteur peut être contacté.

## 7. Analyse et traitement

### 7.1. Accusé de réception et délais

Un accusé de réception écrit est adressé à l'auteur dans un délai de sept jours ouvrés à compter de la réception du signalement lorsqu'il dispose d'un moyen de contact utilisable, sous réserve des exceptions légalement prévues. Il confirme la bonne réception et le numéro de dossier sans préjuger du caractère fondé des faits.

L'auteur joignable reçoit, dans un délai raisonnable n'excédant pas trois mois à compter de l'accusé de réception, les informations écrites sur les mesures envisagées ou prises pour évaluer l'exactitude des faits et, le cas échéant, y remédier, ainsi que sur leurs motifs. En l'absence d'accusé de réception, le délai de trois mois est calculé à partir de l'expiration d'une période de sept jours ouvrés suivant le dépôt, conformément au décret applicable. Ce retour d'information n'implique pas que toutes les investigations ou mesures correctives soient achevées à cette date.

En cas d'absence de coordonnées et d'impossibilité de communication via l'outil, les diligences réalisables sont néanmoins effectuées et l'impossibilité matérielle d'adresser le retour est documentée.

### 7.2. Première analyse

Le référent habilité, ou la personne chargée du tri préalable, examine sans délai excessif le périmètre de l'alerte, les éléments objectifs disponibles, la situation de l'auteur au regard des conditions légales pertinentes lorsqu'elle est connue, l'existence de personnes exposées, le caractère urgent, le risque de représailles, l'existence de conflits d'intérêts et la nécessité éventuelle de mobiliser d'autres compétences.

Une erreur de catégorie, l'absence de pièces ou le choix de ne pas divulguer son identité ne justifient pas un rejet automatique. Si le dossier est incomplet mais suffisamment identifiable pour poursuivre, les précisions utiles sont demandées à l'auteur joignable. Si la situation relève davantage de l'écoute, d'une réclamation RH ordinaire ou d'un autre dispositif, l'auteur est orienté vers l'interlocuteur adéquat lorsque cela est possible ; la transmission d'informations sensibles à cette personne reste soumise aux règles de confidentialité et de nécessité.

Si les conditions légales propres au régime des lanceurs d'alerte ne sont pas remplies, l'auteur en est informé, lorsqu'il est joignable, avec les raisons et les suites retenues. Les faits qui appellent une action au titre d'une autre obligation du Groupe (santé, sécurité, droit du travail, données, etc.) peuvent néanmoins être traités dans ce cadre adapté.

### 7.3. Vérifications et instruction

Les vérifications peuvent comprendre une analyse des documents, une demande d'informations complémentaires, des échanges confidentiels avec les personnes ou témoins utiles, la consultation proportionnée de documents internes, l'intervention de RH, RSE, juridique, sécurité de l'information ou d'un expert externe. Un traitement

approfondi ou un groupe restreint peut être constitué pour un dossier complexe, sensible ou transverse, avec des droits d'accès documentés.

L'instruction respecte l'impartialité, la confidentialité, la nécessité et la proportionnalité de la collecte, les droits des personnes concernées et les règles de preuve applicables. La personne visée conserve ses droits ; aucune sanction n'est fondée sur une simple allégation non vérifiée. Les éléments de nature à identifier l'auteur du signalement ne sont pas communiqués sans son consentement, sauf exceptions prévues par la loi, notamment dans certaines communications à l'autorité judiciaire.

### 7.4. Information pendant l'instruction

Les échanges avec l'auteur portent sur les besoins de précision, les mesures en cours ou envisagées et l'éventuelle poursuite du traitement. Le retour sous trois mois ne comporte ni dossier d'enquête intégral, ni données nominatives de tiers ou mesures individuelles qui ne peuvent légalement être divulguées. La relation avec l'auteur est maintenue lorsque cela est possible et utile, notamment si l'enquête se poursuit au-delà du premier retour.

## 8. Protection des personnes et mesures temporaires

Aucune personne ne peut faire l'objet de représailles en raison d'un signalement de bonne foi, d'un témoignage, d'une demande de soutien ou d'une participation légitime au traitement d'une alerte. Les représailles peuvent notamment prendre la forme d'une sanction, d'une mise à l'écart, d'un refus d'évolution, d'une mesure défavorable, d'une intimidation ou d'un harcèlement. Elles peuvent être signalées par le dispositif.

Dès que des éléments font apparaître un risque important ou immédiat pour la santé, la sécurité, la dignité, les données ou la conservation des preuves, le référent habilité fait évaluer sans attendre la clôture la nécessité de mesures temporaires. En matière sociale, les fonctions RH compétentes et les référents harcèlement de l'entité concernée interviennent selon leurs responsabilités et uniquement si elles ne sont pas impliquées dans les faits.

Les mesures adaptées peuvent notamment comprendre la limitation temporaire des contacts, un aménagement de l'organisation du travail ou de l'affectation à une mission, un soutien RH ou psychologique, l'orientation vers la médecine du travail, la préservation de documents ou un rappel du principe de non-représailles. Une mesure nécessitant une autorité particulière est approuvée par le décideur compétent, sans transmission inutile d'identités ou de pièces. Ces mesures sont proportionnées, préventives et ne préjugent pas de la réalité des faits.

Lorsque le signalement concerne des tiers externes, les mesures de protection ou de prévention peuvent également être appréciées au regard des relations contractuelles, de la protection de données, de la sécurité ou des risques pour les personnes concernées.

## 9. Mesures correctives et clôture

À l'issue des vérifications, le référent habilité documente une conclusion proportionnée aux éléments disponibles : faits établis ou partiellement établis, faits non établis ou insuffisamment étayés, dossier hors périmètre, signalement devenu sans objet, ou autre issue justifiée. L'absence d'éléments suffisants ne conduit pas à qualifier le signalement de malveillant.

Lorsqu'un manquement, un dysfonctionnement ou un risque est identifié, les mesures appropriées sont décidées par les fonctions compétentes : correction de pratiques ou de procédures, renforcement du contrôle, adaptation organisationnelle, sensibilisation, action technique ou de sécurité, mesures de protection et, lorsque les conditions sont réunies, mesures disciplinaires ou contractuelles. Pour les atteintes aux droits humains et les situations concernant un fournisseur ou partenaire, le traitement prend en compte la cessation du risque, la protection des personnes concernées et les suites adaptées de la relation professionnelle.

Le référent documente la décision, les responsables d'action, les échéances et, lorsqu'il y a lieu, la preuve de réalisation. Lorsque les vérifications nécessaires ont été accomplies et les suites appropriées arrêtées, le dossier est clôturé. Pour une affaire sensible, grave ou impliquant la Direction, la clôture associe les fonctions ou l'instance décisionnaire compétentes, en dehors de tout conflit d'intérêts.

L'auteur joignable est informé par écrit de la clôture selon les dispositions applicables, sans divulgation de données ou de décisions individuelles confidentielles. La clôture du dossier n'interrompt pas le suivi des mesures correctives encore en cours ni la vigilance contre d'éventuelles représailles.

## 10. Registre, suivi et reporting

Un registre sécurisé des signalements est tenu pour assurer la traçabilité et le suivi des délais, sans devenir un duplicata de la totalité des dossiers. Il comporte, dans la mesure nécessaire : numéro unique, date et canal de réception, type de parcours, catégorie, entité éventuellement concernée, niveau d'urgence, référent habilité, dates des accusés et retours, statut, existence de mesures de protection, mesures correctives et échéances, date de clôture et motif général de clôture.

Les narratifs détaillés, pièces jointes, identités et échanges confidentiels sont conservés dans l'espace sécurisé du dossier, et non dans le registre transversal de pilotage. Toute donnée de suivi susceptible de permettre une identification indirecte, notamment dans les petites entités, reste soumise à une limitation de visibilité appropriée.

Chaque référent met à jour les éléments de suivi des dossiers dont il a la responsabilité. La Cheffe de projet RSE consolide uniquement les données de pilotage nécessaires. Le CIO / CDO assure le fonctionnement technique de l'outil sans droit

d’accès transversal au contenu. La Direction et le Comité RSE reçoivent un reporting agrégé ne permettant pas d’identifier les personnes concernées.

Les indicateurs suivis peuvent comprendre le volume et la typologie des signalements, la répartition entre canaux internes et externes, les dossiers clôturés, les délais de réception et de retour, les incidents confirmés, les mesures de protection et de correction, les éventuelles réclamations relatives aux conditions de travail et les sujets pertinents pour les obligations de reporting du Groupe. Les incidents de harcèlement, de discrimination, d’intégrité, de droits humains, de travail forcé / travail des enfants et de sécurité de l’information peuvent être distingués lorsque les données le permettent sans risque de réidentification. Les périodes sans signalement ou sans incident confirmé sont également documentées.

## 11. Protection des données, confidentialité et sécurité

### 11.1. Confidentialité et habilitations

Les données de l’auteur, des personnes mises en cause, des témoins et de tout tiers mentionné, ainsi que les informations recueillies, sont traitées de manière strictement confidentielle. L’accès est limité aux personnes identifiées et habilitées selon le besoin d’en connaître. Les habilitations, leur revue et les journaux d’accès sont documentés. Des garanties de confidentialité et d’impartialité s’appliquent à tout intervenant interne ou externe.

Le consentement de l’auteur est requis pour communiquer les éléments permettant de l’identifier, sous réserve des exceptions légales, notamment lorsque la communication à l’autorité judiciaire est obligatoire. L’auteur est alors informé selon les règles applicables, sauf risque de compromettre la procédure judiciaire.

### 11.2. Séparation des rôles et sécurité technique

L’administration des outils et des accès est distincte de l’analyse du fond. Le CIO / CDO ou les administrateurs techniques ne bénéficient pas, à ce seul titre, de la lecture généralisée des signalements. Une éventuelle intervention technique nécessitant un accès exceptionnel au contenu ou à des métadonnées sensibles doit être préalablement justifiée, autorisée, limitée dans le temps et le périmètre, enregistrée dans les journaux et soumise à des engagements de confidentialité. Le DPO ou la personne chargée de la protection des données est associé, lorsque cela est pertinent, au contrôle de ces accès.

Pour les canaux numériques, les mesures de sécurité portent notamment sur les droits d’accès, la transmission et le stockage sécurisés, la protection des pièces jointes, la gestion des incidents, la journalisation pertinente, les sauvegardes et la sécurisation des échanges avec les personnes externes. La configuration de la page Web est examinée sous l’angle des cookies, traceurs, adresses IP et autres métadonnées susceptibles de compromettre une démarche sans identification nominative.

### 11.3. Information, minimisation et traductions

Une information relative au traitement des données personnelles est rendue accessible avant le dépôt, tant sur l'Intranet que sur le site Internet : finalités, responsable du traitement, fondements, destinataires, conservation ou critères de durée, droits des personnes et modalités d'exercice. Les données recueillies restent pertinentes et limitées au nécessaire ; une pièce sensible sans rapport avec les faits ne doit pas être conservée ou partagée inutilement.

Lorsque l'auteur s'exprime dans une langue autre que le français, le traitement ou la traduction nécessaires sont assurés en respectant les mêmes conditions de confidentialité et de sécurité que le dossier initial. Le recours à un prestataire numérique ou à un sous-traitant donne lieu aux vérifications et engagements contractuels prévus par le RGPD. La nécessité de procéder à une analyse d'impact relative à la protection des données (AIPD) est évaluée et documentée en fonction des risques du dispositif.

### 11.4. Conservation et suppression

Les données relatives à un signalement sont conservées sous une forme identifiante pendant une durée strictement nécessaire et proportionnée au traitement, à la protection des personnes concernées et aux éventuelles investigations complémentaires. Elles peuvent rester en base active jusqu'à la décision définitive sur les suites à donner au signalement ; au-delà, seules les données justifiant une conservation intermédiaire, notamment au titre d'une obligation ou d'un contentieux, sont conservées dans des conditions d'accès restreintes et pour une durée documentée.

Les données inutiles sont supprimées ou anonymisées conformément aux règles applicables. Les données véritablement anonymisées peuvent être conservées à des fins statistiques ou de suivi sans possibilité de réidentifier les personnes. Aucun délai unique de cinq ans n'est appliqué indistinctement à l'ensemble des signalements.

## 12. Signalements auprès d'autorités externes

L'utilisation du dispositif Ailancy n'est pas un préalable obligatoire à toute saisine d'une autorité externe compétente lorsque les conditions prévues par la réglementation sont remplies. Selon la nature des faits et la juridiction concernée, une personne peut notamment s'adresser aux autorités désignées par les textes applicables, telles que la CNIL pour les données personnelles, l'Agence française anticorruption pour certaines atteintes à la probité, le Défenseur des droits ou les autorités compétentes en matière de travail, de sécurité et d'environnement.

Les informations utiles sur les autorités habilitées et leurs compétences sont disponibles dans les textes en vigueur, notamment la liste prévue par le décret n° 2022-1284 du 3 octobre 2022 dans sa version applicable. Les voies de divulgation publique, lorsqu'elles sont légalement admises, obéissent à des conditions distinctes.

Pour les entités situées hors de France, il convient de se référer aux autorités et aux exigences du droit local applicable.

Le canal « Alerte professionnelle » publié sur le site d'Ailancy reste, pour sa part, un canal de signalement auprès du Groupe : il ne doit pas être présenté comme une autorité externe indépendante.

## 13. Communication, sensibilisation et révision

Un espace permanent « Alerte & écoute » est mis à disposition sur l'Intranet et une page publique présente les canaux accessibles aux parties prenantes externes. La communication est organisée par la fonction Communication, en lien avec l'équipe RSE. Les supports expliquent simplement les deux parcours, les conditions de confidentialité, l'absence de représailles, la possibilité de ne pas renseigner son identité, les limites liées au choix du canal et les délais de traitement applicables.

Les référents et personnes habilitées reçoivent une sensibilisation adaptée à leurs responsabilités : réception sécurisée, tri et orientation, traitement impartial, conflits d'intérêts, protection des personnes, urgences, délais légaux, documentation, droits des personnes concernées et protection des données. Ces sensibilisations ainsi que les habilitations accordées sont documentées.

Le Comité RSE procède à une revue périodique sur la base des informations agrégées et anonymisées : volume des dossiers, respect des délais, adéquation des référents, incidents et mesures correctives, accessibilité interne et externe, difficultés d'orientation et améliorations techniques nécessaires. Les règles et les contenus des formulaires sont révisés lorsque des évolutions légales, organisationnelles ou techniques le nécessitent. Toute modification significative de la présente procédure est soumise à la validation du Comité RSE.

Lors de toute mise à jour du formulaire ou du tableau des référents, l'équipe RSE veille à la cohérence entre les textes publiés, les droits réellement configurés et les modalités effectives de traitement. Un canal n'est annoncé comme opérationnel que lorsque son fonctionnement et ses garanties de confidentialité ont été vérifiés.