POLITIQUE

DISPOSITIF D'ALERTE PROFESSIONNELLE

(mise à jour de la Politique Dispositif d'Alerte Professionnelle éditée en Septembre 2018 – dernière mise à jour en Mars 2023)

Sommaire

1. Introduction

1.1. Objectifs

Conformément à ses valeurs – ***le Respect des personnes, des lois et de l'environnement*** – et dans le cadre de la mise en place de démarches cohérentes avec son Code d'éthique et sa *Politique Anti-Corruption et Anti-Trafic d'influence,* Verallia a mis en place un **Dispositif d'Alerte professionnelle interne** conformément aux dispositions du III de l'article 8 et de l'article 17 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 (« Loi Sapin 2 ») telle que modifiée par la loi n°2022-401 du 21 mars 2002 et son décret d'application[1] (ci-après ensemble la « **Réglementation** »).

Le Dispositif d'Alerte professionnelle permet à tout Collaborateur ou Partenaire de Verallia de signaler de bonne foi les faits susceptibles d'être contraires aux obligations légales et/ou au Code d'éthique et/ou à la Politique Anti-Corruption et Anti-Trafic d'influence du Groupe Verallia, dans les conditions définies ci-dessous.

Verallia attend de ses Collaborateurs et de ses Partenaires d'agir conformément aux lois, aux codes, aux normes professionnelles, ainsi qu'aux directives, politiques et procédures applicables.

Ce Dispositif d'alerte interne fait partie intégrante du Programme de Conformité de Verallia.

1.2. Définitions

- **Alerte professionnelle /Alerte** : désigne tout signalement transmis par un Lanceur d'alerte, relatif à (i) une violation du Code d'éthique, de la Politique Anti-Corruption et Anti-Trafic d'Influence du Groupe Verallia et plus généralement sur (ii) toute information portant sur un crime ou un délit, une menace ou un préjudice pour l'intérêt général, une violation ou une tentative de dissimulation d'une violation d'un engagement international régulièrement ratifié ou approuvé par la France ou autre pays dont la législation s'applique à Verallia, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, du droit de l'Union européenne, de la loi ou du règlement, ou une menace ou un préjudice pour l'intérêt général. Lorsque les informations n'ont pas été obtenues dans le cadre des activités professionnelles, le Lanceur d'alerte doit en avoir eu personnellement connaissance.

- **Autorité** : désigne toute autorité nationale désignée pour recevoir, suivre et traiter des Signalement externes étant entendu que s'agissant de la France il s'agit (i) des autorités expressément autorisées à recueillir et traiter une Alerte, (ii) du Défenseur des droits, (iii) de l'autorité judiciaire ou (iv) de l'institution, l'organe ou l'organisme de l'Union Européenne compétent pour recueillir des informations sur des violations relevant du champ d'application de la directive (UE) 2019/1937 du Parlement Européen et du Conseil

[1] Décret n° 2022-1284 du 3 octobre 2022 relatif aux procédures de recueil et de traitement des signalements émis par les lanceurs d'alerte et fixant la liste des autorités externes instituées par la loi no 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte.

du 23 octobre 2019. Les Autorités nationales compétentes figurent en Annexe du présent document.

- **Collaborateur :** désigne une personne physique, dirigeant ou membre du personnel d'une entité de Verallia, en poste ou dont la relation de travail s'est terminée, tel qu'un salarié (CDD et CDI), un apprenti, un stagiaire, ou candidat à un emploi au sein de Verallia lorsque les informations ont été obtenues dans le cadre de leur relation avec Verallia.

- **Direction Générale** : désigne le Directeur Général, le Directeur RSE & Juridique Groupe et le Directeur des Ressources Humaines Groupe.

- **Dispositif d'alerte** : désigne l'ensemble des canaux et mesures mis en place au sein de Verallia pour permettre le recueil et le traitement en interne des Alertes professionnelles conformément à la présente Politique Dispositif d'Alerte professionnelle. Trois canaux de remontée des Alertes sont mis à disposition des Collaborateurs et Partenaires : la Voie hiérarchique, la Plateforme et la Ligne Téléphonique. Le Dispositif d'alerte interne n'est qu'un moyen de signalement parmi d'autres.

- **Divulgation :** désigne la mise à disposition d'une Alerte dans la sphère publique (ex. : publication par voie de presse, réseaux sociaux) effectuée par un Lanceur d'alerte dans le respect de la Réglementation.

- **Facilitateur :** désigne toute personne physique ou morale de droit privé à but non lucratif qui aide un Lanceur d'alerte à effectuer une Alerte ou une Divulgation dans le respect de la Réglementation et dont l'aide devrait être confidentielle.

- **Groupe Verallia** : désigne Verallia S.A., de nationalité française, ainsi que toute société contrôlée[2] par Verallia S.A.

- **Lanceur d'alerte** : désigne tout Collaborateur ou Partenaire, personne physique, qui signale ou divulgue sans contrepartie financière directe et de bonne foi une Alerte.

- **Ligne Téléphonique :** désigne la ligne téléphonique mise en place par Verallia et opérée par le prestataire Convercent permettant d'émettre une Alerte oralement. Le recours à la Ligne Téléphonique est facultatif.

- **Mesure de représailles** : désigne tout acte ou omission, direct ou indirect (en ce inclus toute menace ou tentative), qui intervient dans un contexte professionnel et qui est suscité par une Alerte ou un Signalement externe ou une Divulgation, et qui cause ou peut causer un préjudice injustifié au Lanceur d'alerte.

- **Partenaire** : désigne les actionnaires, associés, titulaires de droits de vote au sein de l'assemblée générale d'une entité du Groupe Verallia, les membres des organes

[2] Au sens de l'article L. 233-3 du Code de commerce de la République Française.

d'administration, direction ou surveillance, les collaborateurs extérieurs et occasionnels de Verallia (ex. consultants, commissaire aux comptes, agent etc), ainsi que les cocontractants d'une entité du Groupe Verallia (ex. clients, fournisseurs, prestataires de services etc), leurs sous-traitants ou, lorsqu'il s'agit de personnes morales, les membres de l'organe d'administration, de direction ou de surveillance de ces cocontractants et sous-traitants ainsi qu'aux membres de leur personnel.

- **Personne en lien avec le Lanceur d'alerte** : désigne toute personne physique, en lien avec un Lanceur d'alerte (ex. collègues, proches), qui risque de faire l'objet de Mesures de représailles dans le cadre de ses activités professionnelles de la part de son employeur, de ses clients ou du destinataire de ses services.

- **Plateforme :** désigne l'outil retenu par Verallia permettant de recueillir par écrit, centraliser et traiter en interne une Alerte. Cette Plateforme vient en complément de la Ligne Téléphonique et de la Voie hiérarchique permettant également aux Collaborateurs et Partenaires d'émettre des Alertes lorsque cela est possible en vertu de la réglementation applicable. Le recours à la Plateforme par le Lanceur d'Alerte est facultatif.

- **Retour d'information** : désigne la communication au Lanceur d'Alerte d'informations sur les mesures envisagées ou prises au titre de suivi et sur les motifs de ce suivi.

- **Signalement externe** : désigne le signalement d'une Alerte effectué par un Lanceur d'alerte auprès d'une Autorité compétente, dans le respect de la réglementation, soit après avoir effectué une Alerte auprès de Verallia, soit directement.

- **Traitement de l'Alerte :** désigne l'ensemble des phases de gestion des Alertes.

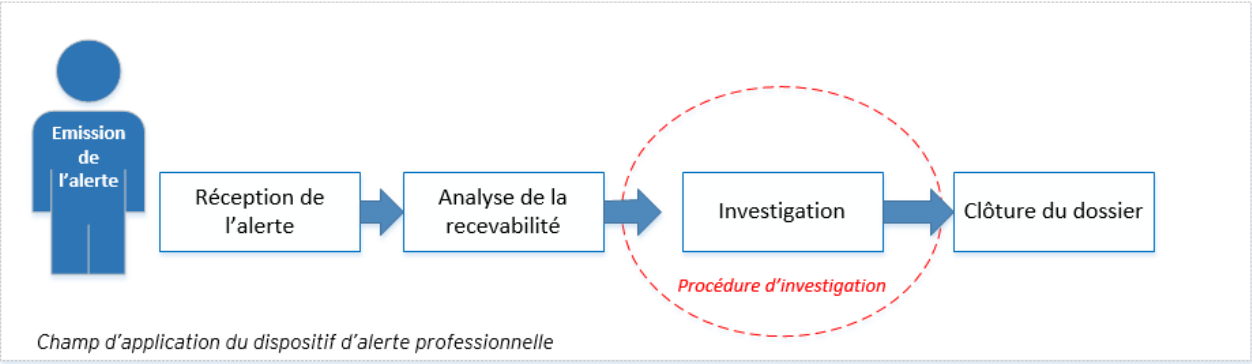
- **Voie hiérarchique** : désigne toute Alerte signalée par un Lanceur d'Alerte (i) à son supérieur hiérarchique, direct ou indirect, ou (ii) à son employeur ou (iii) au référent désigné par l'employeur (v) ou adressée par courrier à l'adresse indiquée à la partie 5 de ce document.

1.3. Champ d'application

Cette politique s'applique à tous les Collaborateurs de Verallia (quel que soit leur rôle, position, département) et les Partenaires, et porte sur le recueil et traitement des Alertes professionnelles par Verallia et plus particulièrement sur leur :

- Emission ;
- Réception ;
- Analyse de la recevabilité ;
- Clôture des Alertes.

La procédure d'investigation des Alertes devant être suivie par les personnes en charge du traitement des Alertes pour le compte de Verallia fait l'objet d'un document distinct (Procédure d'Investigation) et n'est donc pas traitée par la présente Politique.



Champ d'application du dispositif d'alerte professionnelle

Le Dispositif d'alerte s'appuie sur les codes de la profession et les réglementations locales applicables et est imposé par la Réglementation.

Le Dispositif d'alerte implique la mise en œuvre d'un traitement de données à caractère personnel dont les modalités sont décrites dans la présente politique à la partie 3.3 « *Protection des données à caractère personnel* ».

Cette politique ne s'applique pas aux Signalements externes et aux Divulgations qui peuvent être effectués par le Lanceur d'Alerte dans les conditions prévues par la Réglementation.

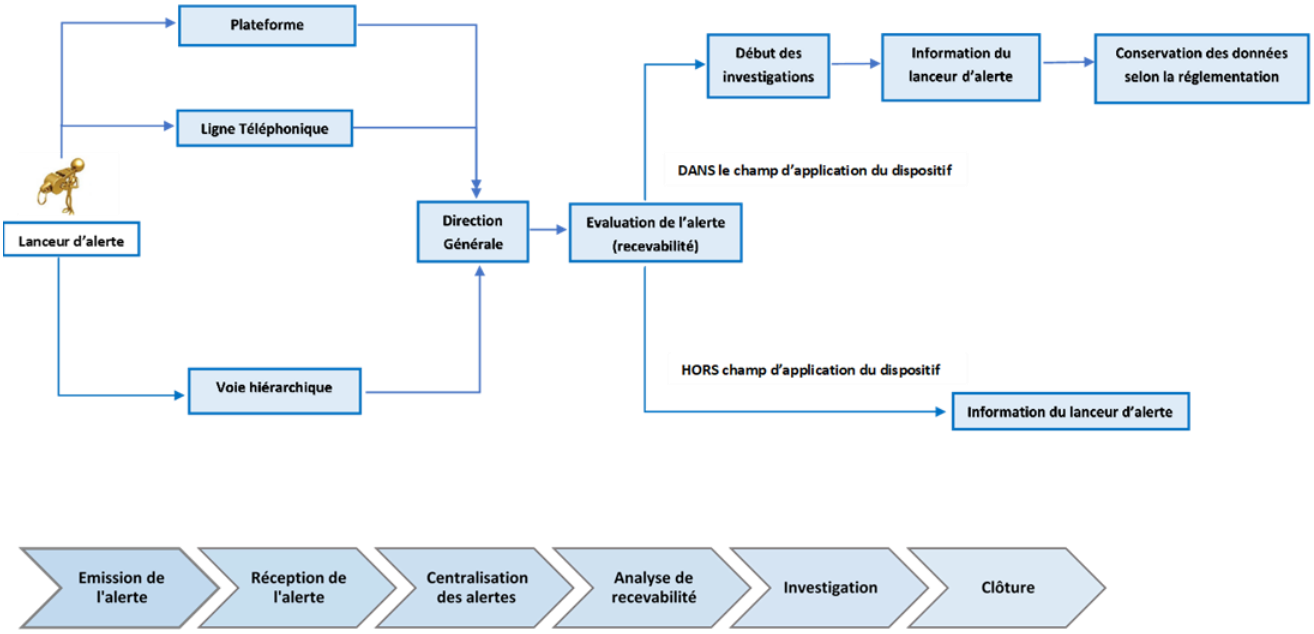
1.4. Rôles et responsabilités

La Direction Générale :

- Réceptionne et centralise les signalements conformément à l'article 2.6 ci-après ;
- Accuse par écrit réception de l'Alerte au Lanceur d'alerte dans un délai de sept (7) jours ouvrés à compter de cette réception ;
- S'assure que le Comité de Triage réalise l'analyse de recevabilité de l'Alerte ;
- Supervise les Investigations, veille à ce que les règles soient respectées ;
- Assure le suivi des mesures prises suite à l'Investigation ;
- Mène régulièrement des actions de sensibilisation de manière à s'assurer que les valeurs de Verallia soient comprises et appliquées par tous les Collaborateurs et Partenaires.

2. Les Alertes professionnelles et le Dispositif d'alerte interne

2.1. Organigramme relatif au Dispositif d'alerte interne



2.2. Quelles Alertes signaler ?

Les Collaborateurs et Partenaires peuvent signaler toute information concernant :

- Une violation du Code d'éthique, de la Politique Anti-Corruption et Anti-Trafic d'influence de Verallia concernant des faits de corruption ou de trafic d'influence ;
- Un crime ou un délit ;
- Une menace ou un préjudice pour l'intérêt général ;
- Une violation ou tentative de dissimulations d'une violation d'un engagement international régulièrement ratifié ou approuvé par la France ou autre pays dont la législation s'applique à Verallia ;
- Une violation ou tentative de dissimulations d'une violation d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, du droit de l'Union européenne, de la loi ou du règlement.

A titre d'illustration, les Alertes peuvent concerner les thématiques suivantes : corruption, pratiques anticoncurrentielles, discriminations, fraude et harcèlement au travail.

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

2.3. Qui peut lancer une Alerte ?

Le Lanceur d'alerte doit être un Collaborateur ou un Partenaire de Verallia (comme défini dans la partie 1.2 « *Définitions* »).

En outre le Lanceur d'alerte doit :

- **Avoir obtenu directement ou indirectement les informations dans le cadre de ses activités professionnelles ou, lorsque ce n'est pas le cas, en avoir eu personnellement connaissance :** le Lanceur d'alerte estime d'une manière raisonnable que les informations qu'il signale sont susceptibles de constituer des informations pouvant être signalées (conformément à la définition à la partie 2.2).
- **Agir sans contrepartie financière directe** : le Lanceur d'alerte doit agir dans le but de défendre l'intérêt général et non pour son propre compte. L'Alerte ne peut avoir pour motivation de nuire à autrui.
- **Agir de bonne foi** : l'utilisation abusive du Dispositif d'alerte peut exposer son auteur à des sanctions disciplinaires ou poursuites judiciaires. Toutefois, l'utilisation de bonne foi du Dispositif d'alerte, même si les faits s'avèrent par la suite inexacts ou ne donnent lieu à aucune suite, n'exposera son auteur (ou les Facilitateurs ou Personnes en lien avec le Lanceur d'Alerte) à aucune Mesure de représailles.

L'utilisation du Dispositif d'alerte est un droit que les personnes concernées exercent librement, son recours reste facultatif. Dès lors, l'absence d'utilisation du Dispositif d'alerte n'entraînera aucune conséquence pour les Collaborateurs et Partenaires.

2.4. Contenu et langue de l'Alerte

De manière générale, et sous réserve de la règlementation localement applicable, l'Alerte peut être faite de manière anonyme ou non.

Cependant, sous réserve que cela ne soit pas interdit en vertu de la règlementation localement applicable, **Verallia encourage le Lanceur d'alerte à révéler son identité**. Cette dernière sera, en toute état cause, protégée et traitée de manière strictement confidentielle dans les conditions prévues à la partie 3.2 « *Confidentialité* ». Par exception, lorsque la gravité des faits est établie et que les faits sont suffisamment détaillés, le signalement peut être effectué de manière anonyme. Toutefois les signalements anonymes ne sont pas encouragés et ne permettent pas un traitement efficient de l'Alerte.

Par ailleurs, le Lanceur d'alerte est informé qu'en cas de signalement fait de manière anonyme, Verallia n'a pas l'obligation d'effectuer le Retour d'informations prévu à l'article 2.6.3 ci-après.

Les Lanceurs d'alerte sont invités à fournir les faits, informations et documents de nature à étayer leur signalement, quel que soit leur forme ou leur support. Ces données, qui doivent être en **lien direct avec l'objet du signalement**, peuvent être les suivantes :

- le motif du signalement ;
- l'identité des personnes visées ;
- tout élément, quel que soit sa forme ou son support, de nature à étayer l'Alerte.

Les formulations utilisées pour décrire la nature des faits signalés doivent faire apparaître leur **caractère présumé**.

A cet égard, seuls seront pris en compte les signalements entrant strictement dans le périmètre couvert par le Dispositif d'alerte, formulés de manière objective, et strictement nécessaires à la vérification des faits allégués.

Les Collaborateurs et Partenaires peuvent utiliser la langue de leur choix pour remonter une Alerte. A réception, l'Alerte pourra être traduite (en anglais), si nécessaire.

Hormis le cas où l'Alerte est anonyme, le Lanceur d'Alerte transmet en même temps que son alerte tout élément justifiant qu'il est bien un Collaborateur ou un Partenaire.

2.5. Comment remonter une Alerte ?

Chaque Collaborateur et Partenaire doit se sentir libre d'échanger sur les modalités d'émission de son Alerte, ainsi que sur son contenu.

Toute question en lien avec l'interprétation du périmètre du Dispositif d'alerte peut être discutée avec le Responsable des Ressources Humaines et/ou le Correspondant Conformité de l'entité Verallia employeur ou cocontractante.

Trois canaux de recueil interne des Alertes sont mis à disposition par Verallia (cf. partie 2.1 « *Organigramme* ») :

- **La Voie hiérarchique** : sous réserve que cela ne soit pas interdit en vertu de la réglementation localement applicable, l'Alerte peut être adressée (i) au supérieur hiérarchique, direct ou indirect, du Lanceur d'Alerte, ou (ii) à l'entité Verallia employeur du Lanceur d'Alerte ou (iii) au référent désigné par celle-ci ou (iv) adressée par courrier à l'adresse indiquée à la partie 5 « *Contacts* » de ce document.

- **Plateforme** : l'Alerte peut également être remontée en utilisant l'outil web mis à disposition (par le prestataire Convercent) à l'adresse : https://ethics.verallia.com/

- **La Ligne Téléphonique** : L'Alerte peut être également faite oralement par le Lanceur d'Alerte en téléphonant gratuitement à un centre d'appel (géré par le prestataire Convercent) dont les coordonnées sont disponibles sur la page d'accueil de la Plateforme. Les Alertes orales sontretranscrites de manière intégrale par écrit par le centre d'appel dans la Plateforme (à travers le formulaire).

  Lorsqu'un signalement est recueilli oralement, le centre d'appel vérifie, sauf si le signalement est anonyme, que l'auteur du signalement est bien un Collaborateur ou Partenaire et que le signalement entre bien dans le périmètre du Dispositif d'alerte. A cette fin, Verallia peut demander tout complément d'information à l'auteur du signalement.

De son côté, le Lanceur d'alerte peut demander l'organisation d'une visioconférence ou d'une rencontre physique au choix du Lanceur d'alerte. Cette visioconférence ou cette rencontre téléphonique, sera organisée au plus tard vingt (20) jours ouvrés après réception de la demande. Toute Alerte recueille dans ce cadre fait l'objet, avec l'accord du Lanceur d'Alerte, d'une retranscription sur la Plateforme.

Le Lanceur d'Alerte peut vérifier, rectifier et approuver la transcription de l'Alerte faite sur la Plateforme.

Sous réserve du respect des règles impératives applicables localement, il est rappelé que le Lanceur d'alerte dispose également des possibilités de signalement suivantes :

- Le Lanceur d'alerte peut faire un **Signalement externe**, soit directement auprès d'une Autorité soit après avoir effectué une Alerte auprès de Verallia.

  Ce Signalement externe peut se faire auprès de (i) l'Autorité compétente, (ii) du Défenseur des droits, (iii) de l'autorité judiciaire, (iv) à une institution, à un organe ou organisme de l'Union Européenne compétent pour recueillir ce Signalement.

- Le Lanceur d'alerte peut faire une **Divulgation** lorsque les conditions suivantes sont remplies :
  (i) après avoir effectué un Signalement externe (précédé ou non d'une Alerte auprès de Verallia), sans qu'aucune mesure appropriée ait été prise en réponse à ce Signalement externe à l'expiration du délai du Retour d'informations par l'Autorité[3] ou, lorsque le Défenseur des Droits, l'Autorité judiciaire ou l'institution, l'organe ou l'organisme de l'Union Européenne compétent a été saisie, à l'expiration d'un délai de six (6) mois[4];
  (ii) en cas de danger grave et imminent[5];
  (iii) Ou lorsque la saisine d'une Autorité ferait encourir au Lanceur d'Alerte un risque de Mesures de représailles ou qu'elle ne permettrait pas de remédier efficacement à l'objet de la divulgation, en raison des circonstances particulières de l'affaire, notamment si des preuves peuvent être dissimulées ou détruites ou si le Lanceur d'Alerte a des motifs sérieux

[3] 3 mois (à compter de l'accusé de réception du signalement par l'Autorité ou à défaut d'accusé de réception, à compter de l'expiration d'un délai de 7 jours ouvrés suivant le signalement) ou 6 mois si les circonstances le requièrent.
[4] A compter de l'accusé de réception du signalement ou, à défaut d'accusé de réception, à compter de l'expiration d'un délai de 7 jours ouvrés suivant le signalement.
[5] Cette condition ne s'applique cependant pas (i) au Lanceur d'alerte qui divulgue publiquement des informations obtenues dans le cadre de ses activités professionnelles en cas de danger imminent ou manifeste pour l'intérêt général, notamment lorsqu'il existe une situation d'urgence ou un risque de préjudice irréversible ou (ii) lorsque la divulgation publique porte atteinte aux intérêts de la défense et de la sécurité nationales.

de penser que l'Autorité peut être en conflit d'intérêts, en collusion avec l'auteur des faits ou impliquée dans ces faits[6].

2.6. Traitement des Alertes

2.6.1. Réception et recevabilité

- **Centralisation des Alertes :** Indépendamment du moyen utilisé pour émettre une Alerte auprès de Verallia (Voie hiérarchique, Plateforme ou Ligne Téléphonique), tous les signalements sont remontés à la Direction Générale et sont traités avec la Plateforme :
  - Si une Alerte est remontée par la Voie hiérarchique, le destinataire de l'Alerte doit immédiatement saisir l'Alerte sur la Plateforme ; en cas de difficulté technique, il conviendra de remonter l'Alerte au Directeur RSE et juridique Groupe et le Responsable Conformité Groupe à l'adresse suivante : compliance@verallia.com ;
  - Si une Alerte vise un ou plusieurs membres de la Direction Générale et/ou un de ses actionnaires, le Lanceur d'alerte ou le destinataire de l'Alerte informe directement le Responsable Conformité Groupe.

- **Réception de l'Alerte :** Si une Alerte est lancée via la Plateforme ou la Ligne Téléphonique**,** un accusé réception est adressé via la Plateforme au Lanceur d'alerte. Si une Alerte est lancée via la Voie hiérarchique, un email de réception est envoyé par le Directeur RSE et Juridique Groupe ou le Responsable Conformité Groupe. Dans tous les cas, cet accusé de réception est adressé par écrit dans un délai de sept (7) jours ouvrés à compter de cette réception. A cet égard, il est précisé que l'accusé de réception ne vaut pas recevabilité du signalement.

- **Recevabilité de l'Alerte :** Chaque Alerte donne lieu à une analyse préliminaire, traitée de manière confidentielle, afin de déterminer si l'Alerte entre dans les domaines présentés à la partie 2.2 « *Quelles Alertes signaler* ? ».
  - Les Alertes ne se rapportant pas aux domaines présentés à la partie 2.2 « *Quelles Alertes signaler* ? » ne peuvent pas être traitées dans le cadre du Dispositif d'alerte ; le Lanceur d'alerte sera informé et orienté vers la voie appropriée ;
  - Les Alertes entrant dans le périmètre du Dispositif seront traitées conformément à la présente Politique.

Le Lanceur d'alerte est informé des raisons pour lesquelles Verallia considère que l'Alerte n'est pas recevable. L'Alerte non-recevable est anonymisée sans délai.

2.6.2. Investigation

Si les faits signalés entrent dans le périmètre du Dispositif d'alerte, l'instruction de l'Alerte est réalisée selon des moyens (entretiens, recherches de données, etc.) qui peuvent varier selon le contexte et la nature du sujet.

[6] Cette condition ne s'applique cependant pas lorsque la divulgation publique porte atteinte aux intérêts de la défense et de la sécurité nationales.

Les Alertes sont traitées par les services internes de Verallia qui ont besoin d'en connaitre, à savoir :

- le Comité de Triage, composé du Directeur Général Groupe, le Directeur RSE & Juridique Groupe, du Directeur des Ressources Humaines Groupe et du Responsable Conformité Groupe ;
- le Comité d'Investigation, composé du Responsable des Investigations et l'équipe d'investigation.
- le Comité Conformité Groupe (dans la mesure strictement nécessaire et proportionnée au regard de la justification de la communication).

Les responsables de l'investigation peuvent prendre contact avec l'entité Verallia locale concernée par les faits, et diverses personnes (salariés, clients, fournisseurs) afin d'obtenir les informations, les données et documents nécessaires au traitement de l'Alerte. Ils peuvent également faire appel à des experts internes et/ou externes à Verallia appropriés (Direction de l'audit interne, Direction des ressources humaines, avocats, expert-comptable, analystes etc.).

Pour tous ces contacts et ces communications, les informations relatives à l'existence et au contenu de l'Alerte ne sont communiquées que dans la limite du strict nécessaire.

Par ailleurs, les formulations utilisées pour décrire la nature des faits signalées font apparaître leur caractère présumé. La personne visée par l'alerte bénéficie en effet pendant toute la durée des investigations de la **présomption d'innocence**.

2.6.3. Communication avec le Lanceur d'alerte – Clôture

Verallia met en œuvre tous les moyens nécessaires pour pouvoir traiter les Alertes dans des délais raisonnables, notamment par le biais d'échanges avec le Lanceur d'alerte pour l'obtention d'informations suffisantes afin d'étudier les faits.

Des informations supplémentaires ou des questions peuvent être posées au Lanceur d'alerte soit via la Plateforme, soit directement en communiquant avec le Lanceur d'alerte, avec son consentement.

Verallia fait un Retour d'informations au Lanceur d'alerte (notamment relativement à la clôture de l'instruction de l'Alerte) dans un délai raisonnable, n'excédant pas trois (3) mois à compter de l'accusé de réception de l'Alerte ou, à défaut d'accusé de réception, trois (3) mois à compter de l'expiration de la période de sept (7) jours ouvrés suivant l'Alerte. A ce titre, Verallia communique par écrit au Lanceur d'alerte des informations sur les mesures envisagées ou prises pour évaluer l'exactitudes des allégations et, le cas échéant, remédier à l'objet du signalement ainsi que sur les motifs de ces dernières.
Le Lanceur d'alerte est informé par écrit de la clôture de l'Alerte.

3. Principes généraux

3.1. Généralités

En émettant une Alerte, les Collaborateurs et Partenaires de Verallia sont informés des principes décrits ci-dessous :

- Les Alertes font l'objet d'un reporting régulier au Comité Conformité ;
- Les Alertes sont traitées par les personnes désignées à cet effet. En toute hypothèse, ces personnes disposent de la compétence, de l'autorité et des moyens suffisants à l'exercice de leurs missions ;
- Le Dispositif d'alerte ne peut fonctionner qu'à partir d'informations communiquées de « bonne foi ».

3.2. Protection du Lanceur d'alerte et des Facilitateurs

Il est rappelé au Lanceur d'alerte que, sous réserve de la réglementation localement applicable :

- Qu'il n'est **pas civilement responsable** des dommages causés du fait de son signalement ou sa divulgation dès lors que son signalement a été fait dans le respect des dispositions applicables et que le Lanceur d'alerte avaient des motifs raisonnables de croire, lorsqu'il y a procédé, que le signalement ou la divulgation publique de l'intégralité de ces informations était nécessaire à la sauvegarde des intérêts en cause.
- Qu'il n'est **pas responsable pénalement** en ce qui concerne l'obtention des informations qui sont signalées ou divulguées publiquement, ou l'accès à ces informations, à condition que cette obtention ou cet accès ne constitue pas, en vertu de la réglementation localement applicable une infraction pénale autonome. Au cas où cette obtention ou cet accès constitue une infraction pénale autonome, les règles de responsabilité pénale applicables localement s'appliquent[7].
- Qu'il **ne peut faire l'objet de Mesure de représailles** pour avoir signalé ou divulgué des informations dans le respect de la Réglementation.

Verallia ne tolère aucune forme de représailles, de menaces ou de tentative de recourir à ces mesures contre les Lanceurs d'alerte, tel que le harcèlement.

[7] *En droit français, en vertu de l'article 122-9 du Code pénal, « N'est pas pénalement responsable la personne qui porte atteinte à un secret protégé par la loi, dès lors que cette divulgation est nécessaire et proportionnée à la sauvegarde des intérêts en cause, qu'elle intervient dans le respect des conditions de signalement définies par la loi et que la personne répond aux critères de définition du lanceur d'alerte prévus à l'article 6 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.*
N'est pas non plus pénalement responsable le lanceur d'alerte qui soustrait, détourne ou recèle les documents ou tout autre support contenant les informations dont il a eu connaissance de manière licite et qu'il signale ou divulgue dans les conditions mentionnées *au premier alinéa du présent article.*
Le présent article est également applicable au complice de ces infractions »

Les Facilitateurs ainsi que les Personnes en lien avec le Lanceur d'alerte et les entités juridiques contrôlées par le Lanceur d'alerte ou pour lesquelles il travaille, sont inclus dans la politique de non-représailles de Verallia et bénéficient des mêmes protections que le Lanceur d'alerte.

Des procédures disciplinaires ou des sanctions civiles ou pénales peuvent être prises contre l'auteur de telles représailles ou contre toute personne qui ne respecte pas les droits du Lanceur d'alerte.

3.3. Confidentialité

Le Traitement de l'Alerte est réalisé en respectant **l'intégrité et la confidentialité** des informations recueillies dans une Alerte, notamment l'identité du Lanceur d'alerte, celle des personnes visées par l'Alerte et de tout tiers qui y est mentionné conformément à la loi applicable.

A cet égard :

- Les personnes désignées pour traiter les Alertes sont les personnes mentionnées à l'article 2.6.2 et 3.4.1 du présent document. L'accès aux informations recueilles dans le cadre de l'Alerte est interdite à toute personne non autorisée à en connaitre.
- Toutes les personnes impliquées dans la gestion des Alertes sont spécialement formées et astreintes à une obligation renforcée de confidentialité. Elles s'engagent notamment, à ne pas utiliser les données à des fins détournées, à respecter la durée de conservation limitée des données conformément à la loi applicable.
- Le Lanceur d'alerte est encouragé à s'identifier, mais son identité est traitée de façon confidentielle par l'organisation chargée de la gestion des Alertes ;
- Les éléments de nature à identifier le Lanceur d'alerte ne peuvent être divulgués qu'avec le consentement de celui-ci[8].
- Les éléments de nature à identifier la personne mise en cause par un signalement ne peuvent pas être divulgués, sauf à l'autorité judiciaire, qu'une fois établi le caractère fondé de l'Alerte.

Dans les limites de leurs attributions, les personnes en charge de la Plateforme peuvent également accéder aux données aux fins d'administration de la Plateforme.

[8] Ils peuvent toutefois être communiqués à l'autorité judiciaire, dans le cas où les personnes chargées du recueil ou du traitement des Alertes sont tenues de dénoncer les faits à celle-ci (par exemple : agressions ou atteintes sexuelles infligés à un (i) mineur ou à (ii) une personne vulnérable (en raison d'une maladie, d'une infirmité, d'une déficience physique ou psychique, d'un état de grossesse)). Le lanceur d'alerte en est alors informé, à moins que cette information ne risque de compromettre la procédure judiciaire. Des explications écrites sont jointes à cette information.

3.4. Protection des données à caractère personnel

3.4.1. Données à caractère personnel

- Le Dispositif d'Alerte Professionnelle est mis en place par Verallia S.A. au sein du Groupe Verallia afin de répondre à ses obligations légales et dans l'intérêt légitime de Verallia de conduire ses activités de façon intègre et éthique s'agissant des faits relevant du Code d'éthique.

- **Catégories de données traitées via le Dispositif d'alerte** : Verallia s'engage à ne traiter que des données adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles ont été collectées. Seules les catégories de données suivantes peuvent être traitées :
  - Identité, fonctions et coordonnées de l'émetteur de l'Alerte professionnelle ;
  - Identité, fonctions et coordonnées des personnes faisant l'objet d'une Alerte et/ou cités dans l'Alerte;
  - Identité, fonctions et coordonnées des personnes intervenant dans le recueil ou dans le traitement de l'Alerte ;
  - Faits signalés ;
  - Eléments recueillis dans le cadre de la vérification des faits signalés ;
  - Compte rendu des opérations de vérification ;
  - Suites données à l'Alerte.

- **Destinataires** : Outre les personnes habilitées à traiter les données dans le cadre de leur mission, Verallia S.A. peut communiquer des données :
  - A l'entité du Groupe Verallia concernée par les faits et/ou aux experts internes et/ou externes à Verallia (Direction des ressources humaines, Directeur de l'audit interne, avocats, expert-comptable, analystes etc.) auxquels Verallia peut faire appel pour les besoins du traitement de l'Alerte.
  - Au (aux) prestataire(s) en charge de la fourniture et de l'exploitation de la Plateforme et de la Ligne Téléphonique.

  Le cas échéant, les données peuvent être transmises à l'autorité judiciaire étant précisé que :

  - Les éléments de nature à identifier le Lanceur d'alerte ne seront transmis à l'autorité judiciaire qu'avec le consentement du Lanceur d'alerte[9],
  - Les éléments de nature à identifier la personne mise en cause par une Alerte ne seront divulgués qu'une fois établi le caractère fondé de l'Alerte.

- **Mesures de protection des données à caractère personnel :** Verallia S.A. prend toutes les précautions utiles pour préserver la sécurité des données tant à l'occasion de leur recueil que de leur communication ou de leur conservation.

[9] Sauf dans le cas prévu en note de bas de page n°8 ci-dessus.

Dans ce cadre, les accès aux traitements de données via la Plateforme s'effectuent par un identifiant et un mot de passe individuels, régulièrement renouvelés, ou par tout autre moyen d'authentification. Ces accès sont enregistrés et leur régularité est contrôlée.

3.4.2. Conservation des données à caractère personnel

Dans le cadre du Dispositif :

- Les enregistrements, transcriptions et documents sont conservés le temps nécessaire au traitement du signalement et à la protection de leurs auteurs, des personnes qu'ils visent et des tiers qu'ils mentionnent conformément aux réglementations applicables ainsi qu'aux règles et procédures Verallia en matière de protection et de conservation.
- Dans ce cadre, les données à caractère personnel sont conservées de la manière suivante :
    - Lorsqu'une Alerte est considérée comme n'entrant pas dans les domaines décrits dans la partie 2.2 « *Quelles alertes remonter ?* », l'Alerte est clôturée et les données la concernant sont anonymisées sans délai ;
    - Lorsqu'aucune suite n'est donnée à une Alerte, les données sont anonymisées après la clôture des vérifications selon les lois et règlements en vigueur ;
    - Lorsque des suites sont données à l'Alerte (c'est-à-dire toute décision prise par Verallia pour tirer des conséquences de l'Alerte tels que plan d'action en interne, adoption ou modification des règles internes, réorganisation des opérations ou des services, prononcé d'une sanction mise en œuvre d'une action en justice etc), les données relatives à l'Alerte sont conservées jusqu'au terme de la procédure et/ou jusqu'à acquisition de la prescription ou épuisement des voies de recours.
    - Les données peuvent être conservées plus longtemps, en archivage impliquant une restriction d'accès, si Verallia en a l'obligation légale (par exemple, pour répondre à des obligations comptables, sociales ou fiscales).

3.4.3. Transfert de données en dehors de l'Union Européenne

Les données personnelles sont hébergées sur la Plateforme en Europe. Toutefois, elles peuvent être transférées (i) par Verallia vers des entités du Groupe Verallia ou tiers immatriculés dans des pays situés tant au sein que hors de l'Espace Economique Européen (EEE) aux fins du traitement de l'Alerte professionnelle ou (ii) par le fournisseur de la Plateforme et de la Ligne Téléphonique pour des besoins de support et maintenance. Cela inclut notamment des pays dont le niveau de protection des données personnelles peut différer de celui garanti au sein de l'EEE.

Verallia s'assure que les transferts de données par Verallia ont lieu en conformité avec la règlementation applicable sur la protection des données personnelles et, si nécessaire, met en place des garanties adéquates de protection, telles que l'adoption des clauses contractuelles types adoptées par la Commission Européenne. Les personnes peuvent obtenir

sur demande (à l'adresse suivante : *donnees.personnelles@verallia.com)* des informations complémentaires concernant les transferts hors EEE.

3.4.4. Droits des personnes

Le Dispositif d'alerte garantit la confidentialité et le respect des droits de chacun dans le traitement des démarches engagées.

Le récipiendaire informe le Lanceur d'alerte dès réception de son signalement conformément à la présente procédure.

De la même manière, la personne ayant fait l'objet d'une Alerte est informée de l'enregistrement, informatisé ou non, de données la concernant. Cette information est délivrée dans un délai d'un (1) mois à la suite de l'émission de l'Alerte sauf si cette information est susceptible de rendre impossible ou de compromettre gravement les objectifs du traitement (par exemple, risque de destruction de preuves relatives à l'Alerte). Dans ce cas, la personne ayant fait l'objet d'une Alerte n'est informée que lorsque le risque est écarté.

Toute personne identifiée dans le cadre de ce Dispositif, qu'il s'agisse du Lanceur d'Alerte ou de la personne ayant fait l'objet d'une Alerte, a le droit d'accéder aux données la concernant. Toute personne identifiée peut également demander, dans les conditions et limites prévues par la réglementation applicable, la rectification, l'effacement de ses données ou s'opposer au traitement (sous réserve que ce droit soit applicable) ou de demander la limitation du traitement.

Concernant les droits de rectification et d'effacement, ceux-ci ne peuvent permettre la modification rétroactive des éléments contenus dans une alerte ou collectées lors de son instruction. Ces droits ne peuvent être exercés que pour rectifier les données factuelles dont l'exactitude matérielle peut être vérifiée par Verallia S.A. à l'appui d'éléments probants et sans que soient effacées ou remplacées les données, même erronées, collectées initialement.

Ces droits peuvent être exercés à l'adresse suivante : *donnees.personnelles@verallia.com*.

Il est toutefois précisé que la personne qui fait l'objet d'une Alerte ne peut en aucun cas obtenir communication, sur le fondement de son droit d'accès, des informations concernant l'identité du Lanceur de l'alerte.

Si la personne concernée considère, après avoir contacté Verallia, que ses droits ne sont pas respectés ou que le traitement n'est pas conforme aux règles de protection des données, elle peut adresser une réclamation auprès de l'autorité de contrôle compétente (la CNIL pour la France).

4. Compte-rendu au Comité de Conformité

Le Responsable Conformité Groupe reporte au Comité Conformité Groupe une fois par an : les Alertes, la gestion, et les actions prises à cet égard, en se limitant aux données strictement nécessaires et proportionnées au regard de la justification de la communication.

5. Contacts

Société : Verallia S.A.
Adresse postale : Tour Carpe Diem – 31, Place des Corolles – 92400 Courbevoie (France)
A l'attention du Responsable Conformité Groupe.
Adresse email : *compliance@verallia.com*

Mars 2023

Emise par la Directrice RSE et Juridique Groupe Wendy Kool-Foulon _____

wendy kool-foulon (22 mars 2023 10:25 GMT+1)

Approuvée par le Directeur Général Patrice Lucas _____

Patrice Lucas (22 mars 2023 17:13 GMT+1)

ANNEXE : LISTE DES AUTORITES EXTERNES NATIONALES

1. FRANCE

1.1. 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 ;

1.2. Services, produits et marchés financiers et prévention du blanchiment de capitaux et du financement du terrorisme :

- Autorité des marchés financiers (AMF), pour les prestataires en services d'investissement et infrastructures de marchés ;
- Autorité de contrôle prudentiel et de résolution (ACPR), pour les établissements de crédit et organismes d'assurance ;

1.3. Sécurité et conformité des produits :

- Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF);
- Service central des armes et explosifs (SCAE) ;

1.4. Sécurité des transports :

- Direction générale de l'aviation civile (DGAC), pour la sécurité des transports aériens ;
- Bureau d'enquêtes sur les accidents de transport terrestre (BEA-TT), pour la sécurité des transports terrestres (route et fer) ;
- Direction générale des affaires maritimes, de la pêche et de l'aquaculture (DGAMPA), pour la sécurité des transports maritimes ;

1.5. Protection de l'environnement :

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

1.6. Radioprotection et sûreté nucléaire :

- Autorité de sûreté nucléaire (ASN) ;

1.7. Sécurité des aliments :

- Conseil général de l'alimentation, de l'agriculture et des espaces ruraux (CGAAER);
- Agence nationale chargée de la sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES) ;

1.8. Santé publique :

- Agence nationale chargée de la sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES) ;
- Agence nationale de santé publique (Santé publique France, SpF) ;
- Haute Autorité de santé (HAS) ;

- Agence de la biomédecine ;
- Etablissement français du sang (EFS) ;
- Comité d'indemnisation des victimes des essais nucléaires (CIVEN) ;
- Inspection générale des affaires sociales (IGAS) ;
- Institut national de la santé et de la recherche médicale (INSERM) ;
- Conseil national de l'ordre des médecins, pour l'exercice de la profession de médecin ;
- Conseil national de l'ordre des masseurs-kinésithérapeutes, pour l'exercice de la profession de masseur- kinésithérapeute ;
- Conseil national de l'ordre des sages-femmes, pour l'exercice de la profession de sage-femme ;
- Conseil national de l'ordre des pharmaciens, pour l'exercice de la profession de pharmacien ;
- Conseil national de l'ordre des infirmiers, pour l'exercice de la profession d'infirmier ;
- Conseil national de l'ordre des chirurgiens-dentistes, pour l'exercice de la profession de chirurgien-dentiste ;
- Conseil national de l'ordre des pédicures-podologues, pour l'exercice de la profession de pédicure- podologue ;
- Conseil national de l'ordre des vétérinaires, pour l'exercice de la profession de vétérinaire ;

1.9. Protection des consommateurs :

- Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) ;

1.10. 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) ;

1.11. Violations portant atteinte aux intérêts financiers de l'Union européenne :

- Agence française anticorruption (AFA), pour les atteintes à la probité ;
- Direction générale des finances publiques (DGFIP), pour la fraude à la taxe sur la valeur ajoutée ;
- Direction générale des douanes et droits indirects (DGDDI), pour la fraude aux droits de douane, droits anti- dumping et assimilés ;

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

1.13. Activités conduites par le ministère de la défense :

- Contrôle général des armées (CGA) ;
- Collège des inspecteurs généraux des armées ;

1.14. Statistique publique :

- Autorité de la statistique publique (ASP) ;

1.15. Agriculture :

- Conseil général de l'alimentation, de l'agriculture et des espaces ruraux (CGAAER) ;

1.16. Education nationale et enseignement supérieur :

- Médiateur de l'éducation nationale et de l'enseignement supérieur ;

1.17. Relations individuelles et collectives du travail, conditions de travail :

- Direction générale du travail (DGT)

1.18. Emploi et formation professionnelle :

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

1.19. Culture :

- Conseil national de l'ordre des architectes, pour l'exercice de la profession d'architecte ;
- Conseil des maisons de vente, pour les enchères publiques ;

1.20. 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 ;

1.21. Intérêt supérieur et droits de l'enfant :

- Défenseur des droits ;

1.22. Discriminations :

- Défenseur des droits ;

1.23. Déontologie des personnes exerçant des activités de sécurité :

- Défenseur des droits.

WHISTLEBLOWING SYSTEM POLICY

(update of the Whistleblowing System Policy published by VERALLIA S.A. in September 2018 – last update in March 2023)

Table of content

1. Introduction

1.1. Objectives

In accordance with Verallia's values – **respect for people, laws and the environment** – and as a part of the implementation of an approach in line with its *Code of Ethics and its Anti-Corruption and Anti-Trading in Influence Policy*, Verallia has implemented an internal **Whistleblowing System** complying with Article 8, paragraph III and Article 17 of the law No. 2016-1691 of December 9, 2016 on transparency, the fight against corruption and the modernization of the Economy ("Loi Sapin 2") as amended by Act No. 2022-401 of March 21, 2002 and its implementing decree[1] (hereinafter together the "**Regulations**").

The Whistleblowing System enables every Verallia Collaborator and Partner to report in good faith actions that potentially contradict the legal obligations, or the Code of *Ethics*, or the Group's Anti-Corruption and Anti-Trading in Influence Policy, under the conditions defined below.

Verallia expects its Collaborators as well as its Partners to act in accordance with the laws, codes, professional standards, as well as applicable directives, policies and procedures.

This internal **Whistleblowing System** constitutes an integral part of Verallia's Compliance Program.

1.2. Definitions

- Professional Alert /Alert : means any report transmitted by a Whistleblower, relating to (i) a violation of the Verallia Group's Code of Ethics, Anti-Corruption and Anti-Influence Trading Policy and, more generally, (ii) any information concerning a crime or misdemeanour, a threat or harm to the general interest, a violation or an attempt to conceal a violation of an international commitment duly ratified or approved by France or another country whose legislation applies to Verallia, of a unilateral act of an international organization taken on the basis of such a commitment, of the law of the European Union, of a law or regulation, or a threat or harm to the general interest. When the information was not obtained in the course of professional activities, the Whistleblower must have had personal knowledge of it.

- **Authority:** means any national authority designated to receive, monitor and process External Alert, it being agreed that in the case of France this means (i) the authorities expressly authorized to collect and process an Alert, (ii) the Defender of Rights , (iii) the judicial authority or (iv) the European Union institution, body or agency competent to collect information on violations falling within the scope of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019. The competent National Authorities are listed in the Annex to this document.

- **Collaborator:** refers to a natural person, director or member of staff of a Verallia entity, in office or whose employment relationship has ended, such as an employee (fixed-term contract and permanent contract), a trainee, an intern or applicant for employment with Verallia when the information was obtained in the course of their relationship with Verallia.

- **General Management**: refers to the Group CEO, the Group CSR & Legal Director and the Group Human Resources Director.

[1] Decree no. 2022-1284 of October 3, 2022 relating to the procedures for collecting and processing whistleblowers' alerts and establishing the list of external authorities instituted by Law no. 2022-401 of March 21, 2022 to improve the protection of whistleblowers.

- **Whistleblowing System:** refers to all channels and measures set up by Verallia in order to enable the internal collection and processing of all professional Alerts in compliance with this whistleblowing system Policy. Three channels for reporting Alerts are available to Collaborators and Partners: through Hierarchical channel, though the Platform and through the Phone Line. The Internal Whistleblowing System is only one of several channels for reporting.

- **Disclosure:** means the provision of an Alert in the public sphere (e.g.: publication in the press, social networks) by a Whistleblower in compliance with the Regulations.

- **Facilitator:** means any natural or legal person under private, non-profit law who assists a Whistleblower in issuing an Alert or Disclosure in compliance with the Regulations and whose assistance should be confidential.

- **Verallia, the Group:** refers to Verallia S.A. (*société anonyme)*, a limited company of French nationality, as well as every entity controlled[2] by Verallia S.A.

- **Whistleblower:** every Employee or Partner, as a natural person, who reports or discloses, without direct financial consideration and in good faith an alert.

- **Phone Line**: refers to the phone line implemented by Verallia and operated by the service provider Convercent enabling to issue an Alert orally. The use of the Phone Line is optional.

- **Retaliation**: means any act or omission, whether direct or indirect (including any threat or attempt), that occurs in a business context and is prompted by an Alert, an External Alert or Disclosure, and that causes or may cause undue harm to the Whistleblower.

- **Partner:** refers to shareholders, associates, holders of voting rights in the general assembly of a Verallia entity, members of administrative, management or supervisory bodies, Verallia's external and occasional staff (consultant, auditor, agent) as well as the co-contractors of a Verallia Group entity (e.g. customers, suppliers, service providers, etc.), their subcontractors or, in the case of legal entities, the members of the administrative, management or supervisory bodies of these co-contractors and subcontractors, as well as the members of their staff.

- **Person in contact with the Whistleblower**: any natural person in contact with a Whistleblower (e.g. colleagues, relatives) who is at risk of retaliatory action in the course of his or her professional activities by his or her employer, clients or recipient of his or her services.

- **Platform:** refers to the tool chosen by Verallia enabling to collect an Alert in writing via an external web platform. This Platform supplements, where applicable, the Phone Line and the Hierarchical channel, which also allows Collaborators and Parners to issue Alerts when possible under the applicable regulations. The use of the Platform is optional.

- **Feedback:** means the communication to the Whistleblower of information on actions being considered or taken as follow-up and the reasons for such follow-up.

[2] Within the meaning of Article L. 233-3 of the French Commercial Code

- **External Alert:** refers to the reporting of an Alert by a Whistleblower to a Competent Authority, in compliance with the regulations, either after having issued an Alert to Verallia, or directly.

- **Treatment of the Alert:** refers to all the steps of the management of the Alerts.

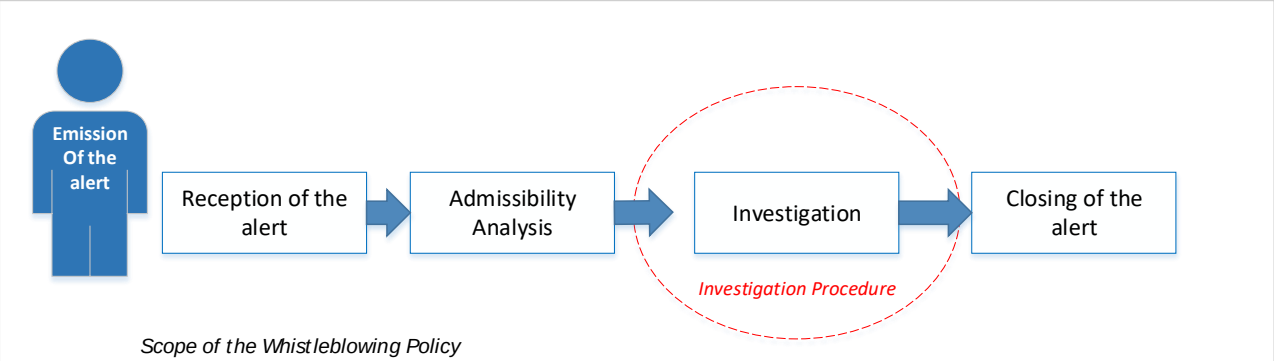
- **Hierarchical channel:** refers to any Alert reported to (i) the direct or indirect line manager of the Whistleblower or (ii) to the employer or (iii) to the compliance correspondent appointed by it or (iv) sent to the postal address mentioned in section 5 of this document.

1.3 Scope

This policy applies to all Verallia Collaborators (regardless of their role, position, department) and Partners. It focuses on the collection and Treatment of Alerts, and covers in particular their:

- Issuance;
- Reception;
- Analysis of admissibility;
- Closing of the Alert.

The procedure for investigating Alerts that must be followed by the persons in charge of processing Alerts on behalf of Verallia is the subject of a separate document (Investigation Procedure) and is therefore not covered by this Policy.



Scope of the Whistleblowing Policy

The Whistleblowing System is based on applicable professional codes and local regulations and is required by the French law.

The System involves the processing of personal data, the procedures for which are described in this policy within the 3.3 " Data protection" section.

This policy does not apply to External Alerts and Disclosures that may be made by the Whistleblower in accordance with the Regulations.

1.4. Roles and Responsibilities

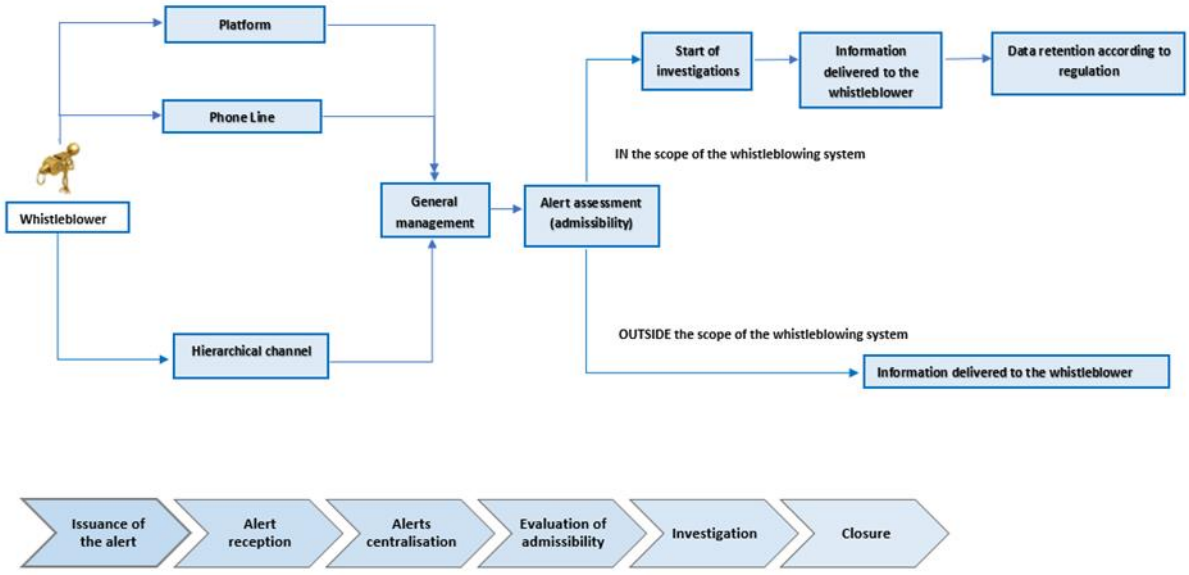
The General Management:

- Receives and centralizes the alerts in accordance with Article 2.6 below;
- Acknowledges in writing receipt of the Alert to the Whistleblower within seven (7) calendar days of such receipt;
- Ensures that the Triage Committee performs the analysis of the admissibility of the Alert;
- Supervises the Investigations, ensuring that the rules are respected;

- Follows up on the measures taken following the Investigation;
- Conducts regular awareness-raising activities to ensure that Verallia's values are understood and applied by all employees and partners.

2. The Alerts and the Internal Whistleblowing System

2.1. Flowchart related to the Internal Whistleblowing System



2.2 Which alerts should be reported?

Collaborators and Partners can report any facts related to:

- Violations of Verallia Code of Ethics and the Anti-Corruption and Anti-Trading in Influence Policy;
- Crimes or offences;
- A threat or injury to the public interest;
- A breach or an attempt to conceal a beach of an international commitment regularly ratified or approved by France or another country whose legislation applies to Verallia;
- A breach or an attempt to conceal a breach of a unilateral act of an international organization taken on the basis of such a commitment, of the law of the European Union, of the law or of the regulations.

As an example, the Alerts can relate to the following subjects: corruption, anti-competitive practices, discrimination, fraud, workplace harassment.
Facts, information and documents, regardless of their form or medium, the revelation or disclosure of which is prohibited by provisions relating to national defense confidentiality, medical confidentiality, the confidentiality of judicial deliberations, the confidentiality of judicial investigations or proceedings, or attorney-client privilege are excluded from this Policy.

2.3. Who can raise an Alert?

The Whistleblower must be a Verallia Collaborator or Partner (as defined in section 1.2 "*Definitions*").

Furthermore, the Whistleblower must:

- **Directly or indirectly have obtained the information in the course of his or her professional activities or, where this is not the case, had personal knowledge of it:** the Whistleblower reasonably believes that the information he or she is reporting is likely to constitute reportable information (as defined in section 2.2).

- Act without direct financial consideration: The Whistleblower must act with the objective to defend the public interest and not in his/her own interest. The Alert can't be motivated by harming others.

-Act in good faith: The misuse of the Whistleblowing System can lead to disciplinary sanctions or judicial proceedings against their author. However, using the Whistleblowing System in good faith, even if the reported information turns out to be inaccurate or does not lead to further proceedings, will not expose the author (or the Facilitators or Persons connected with the Whistleblower) to any Retaliatory Action.

Making use of the Whistleblowing System is a right that the persons concerned can freely exercise, its use remains optional. Therefore, not using the Whistleblowing System will not have any consequences for Collaborators and Partners.

2.4 Content and language of Alerts

In general, and subject to locally applicable regulations, the Alert may be made anonymously or not.

However, provided that it is not prohibited under locally applicable regulations, **Verallia encourages the Whistleblower to disclose his/her identity**. In any case, the identity will be protected and treated in a strictly confidential manner according to the conditions set out in section 3.2 "Confidentiality". By way of exception, if the seriousness of the facts is established and the facts are sufficiently detailed, Alerts can be made anonymously. However, anonymous reports are not encouraged and do not allow an efficient processing of the Alert.

Furthermore, the Whistleblower is informed that in the event of an anonymous report, Verallia is not obliged to provide the feedback provided for in article 2.6.3 below.

Whistleblowers are advised to provide the facts, information and documents to support their Alert, regardless of their form or medium. This data, which must **be directly related to the subject of the alert** , may include the following:

- The reason for raising the Alert;
- The identity of the persons subject to the Alert;
- Any item of information in any form or medium, considered necessary to support the Alert.

The wording used to describe reported facts must reflect their **alleged nature**.

In this context, the only Alerts that will be taken into account are those strictly limited to the facts covered by the Whistleblowing Policy, formulated in an objective manner and strictly necessary for the verification of the allegations.

Collaborators and Partners can choose in which language they would like to make the Alert. Upon receipt, the Alert can be translated (into English) if necessary.
Except in the case where the Alert is anonymous, the Whistleblower transmits at the same time as his alert any element justifying that he is indeed a Collaborator or a Partner.

2.5. How to raise an Alert?

Every employee must feel free to discuss about the ways to raise an Alert as well as its content.

Any question related to the interpretation of the scope of the Whistleblowing process can be discussed with the Head of Human Resources and/or the Compliance correspondent of the employing or subcontracting Verallia entity.

Three channels for reporting Alerts are available (see section 2.1 "*Flow Chart*"):

- **The Hierarchical channel**: provided that this is not prohibited under locally applicable regulations, the Alert can be reported (i) to the direct or indirect line manager or (ii) to the employing Verallia entity or (iii) to the Compliance correspondent appointed by it or (iv) by sending a letter to the postal address mentioned in section 5 "Contact" of this document.

- **Platform**: The Alert can also be made by using the web tool (Whistleblowing Platform Convercent) available at the following link: https:// Ethics.Verallia.com.

- **Phone Line:** the Alert can also be made orally by phoning free of charge to a call centre (managed by the Convercent service provider) whose contact details are available on the Platform's homepage. Oral Alerts are transcribed in writing by the call centre (through the form).

  When a report is received verbally, the call center verifies, unless the report is anonymous, that the author of the report is indeed an Employee or Partner and that the report falls within the scope of the Alert System. To this purpose, Verallia may request any additional information from the author of the alert.

  For his or her part, the whistleblower may request the organization of a videoconference or a physical meeting of the whistleblower's choice. This videoconference or telephone meeting will be organized no later than twenty (20) days calendar after receipt of the request. Any Alert collected within this framework is subject, with the agreement of the Whistleblower, to a transcription on the Platform.

The Whistleblower can verify, rectify and approve the transcription of the Alert made on the Platform.

Subject to compliance with the imperative rules applicable locally, it is recalled that the Whistleblower also has the following reporting options:

- The Whistleblower can make an **External Alert**, either directly to an Authority or after having issued an Alert to Verallia.

  This **External Alert** may be made to (i) the competent Authority, (ii) the Defender of Rights, (iii) the judicial authority, (iv) an institution, body or organization of the European Union competent to receive this Alert.

- The Whistleblower may make a **Disclosure** when the following conditions are met:

(i) after having made an External Alert (whether or not preceded by an Alert to Verallia), without any appropriate action having been taken in response to this External Alert at the expiration of the deadline for the Return of Information by the Authority[3] or, when the Defender of Rights, the Judicial Authority or the competent European Union institution, body or agency has been seized, at the expiration of a period of six (6) months[4];

(ii) in case of serious and imminent danger[5];

(iii) Or where referral to an Authority would put the Whistleblower at risk of Retaliatory Action or would not effectively address the subject matter of the disclosure, due to the particular circumstances of the case, including where evidence may be withheld or destroyed or where the Whistleblower has substantial reason to believe that the Authority may have a conflict of interest in collusion with the instigator of the facts or involved in these facts.[6]

2.6. Management of Alerts

2.6.1 Reception and admissibility

- **Centralisation of the Alerts:** Regardless of the channel used to make an Alert to Verallia (Hierarchical channel, Platform or Phone Line), all Alerts are reported to the General Management and treated through the Platform:
  - If an Alert is reported by using the Hierarchical channel, the receiver of the Alert has to immediately report the Alert on the Platform; in the event of technical difficulties, the Alert should be transmitted to the Group CSR and Legal Director and the Group Compliance Officer at the following address : compliance@verallia.com ;
  - If an Alert relates to one or more members of the General Management and/or one of its shareholders, the Whistleblower or the recipient of the Alert shall directly inform the Group Compliance Officer.

- **Receipt of the Alert**: If an Alert is launched via the Platform or the Telephone Line, an acknowledgement of receipt is sent via the Platform to the Whistleblower. If an Alert is launched via the hierarchical channel, an email of receipt is sent by the Group CSR and Legal Director or the Group Compliance Officer. In all cases, this acknowledgement of receipt is sent in writing within seven (7) calendar days of receipt. In this respect, it is specified that the acknowledgement of receipt does not constitute the admissibility of the report.

[3] 3 months (from the acknowledgement of receipt of the alert by the Authority or, in the absence of such acknowledgement, from the expiration of a period of 7 calendar days following the alert) or 6 months if the circumstances so require.
[4] From the acknowledgement of receipt of the report or, in the absence of acknowledgement of receipt, from the expiration of a period of 7 calendar days following the report.
[5] This condition does not apply, however, (i) to a Whistleblower who publicly discloses information obtained in the course of his or her professional activities in cases of imminent or obvious danger to the public interest, in particular where there is an emergency situation or a risk of irreversible harm, or (ii) where the public disclosure is prejudicial to the interests of national defense and security.
[6] This condition does not apply, however, when the public disclosure affects the interests of national defense and security.

- **Admissibility of the Alert:** Each Alert is subject to a preliminary analysis, is treated in a confidential manner, to determine whether the Alert falls within the scope of section 2.2 "*What should be reported?*"

  - The Alerts out of the scope of section 2.2 "Which alerts should be reported?" cannot be treated within the Whistleblowing System; the Whistleblower will be notified and guided towards the appropriate channels.
  - The Alerts within the scope of the Whistleblowing System will be treated in accordance with this Policy.

The Whistleblower is informed of the reasons why Verallia considers that the Alert is not admissible. The non-receivable Alert is anonymized without delay.

2.6.2 Investigation

If the facts reported are within the scope of the Whistleblowing System, the investigation of the Alert is carried out using means (interviews, data searches, etc.) that may vary depending on the context and the nature of the subject.

Alerts are processed by Verallia's internal departments that need to know them, namely:

- the Triage Committee, made up of the Group CEO, the Group CSR & Legal Director, the Group Human Resources Director and the Group Compliance Officer;
- the Investigation Committee, made up of the Head of Investigation and the investigation team.
- the Group Compliance Committee (to the extent strictly necessary and proportionate with regard to the justification for supplying the information).

The Head of Investigation may contact the local Verallia entity concerned by the facts, as well as various persons (employees, customers, suppliers) in order to obtain the information, data and documents necessary to process the Alert. They may also call on the appropriate internal and/or external experts (internal audit department, human resources department, lawyers, chartered accountants, analysts, etc.).

For all these contacts and communications, information relating to the existence and content of the Alert is only communicated to the extent strictly necessary.
Furthermore, the wording used to describe reported facts should reflect their alleged nature. The person targeted by the Alert is **presumed innocent** throughout the investigations.

2.6.3 Communication with the Whistleblower - Closure

Verallia implements all the necessary means to treat the Alerts within a reasonable delay, including by communicating with the Whistleblower in order to obtain sufficient information to analyse the reported facts.

Additional information can be requested or questions can be asked to the Whistleblower either via the Whistleblowing tool, or by communicating directly with the Whistleblower if he/she agrees to do so.

Verallia shall provide the Whistleblower with feedback (in particular with regard to the closure of the investigation of the Alert) within a reasonable period of time, not exceeding three (3) months from the acknowledgement of receipt of the Alert or, in the absence of an acknowledgement of receipt, three (3) months from the expiration of the period of seven (7) calendar days following the Alert. In this

respect, Verallia will provide the Whistleblower with written information on the measures planned or taken to assess the accuracy of the allegations and, if applicable, to remedy the subject of the alert, as well as the reasons for such measures.

The Whistleblower is notified by writing about the closing of the treatment of the Alert.

3. General Principles

3.1. General

When raising an Alert, Verallia Collaborators and Partners are informed of the following principles:

- The Alerts are subject to regular reporting to the Compliance Committee;
- The Alerts are treated by persons designated for this task. In any case, these people have the competency, the authority and the means to carry out their missions;
- The Whistleblowing System can only work with information communicated in "good faith".

3.2 Protection of Whistleblowers and Facilitators

The Whistleblower is reminded that, subject to locally applicable regulations:

- He or she **is not under civil liability** for damages caused by his or her reporting or disclosure if the reporting was done in accordance with the applicable provisions and the Whistleblower had reasonable grounds to believe, when he or she did so, that the reporting or public disclosure of all such information was necessary to protect the interests at stake.
- He or she **is not criminally liable**[7] for obtaining or accessing publicly reported or disclosed information, provided that such obtaining or accessing does not constitute an autonomous criminal offence under the locally applicable regulations. In the event that such obtaining or access constitutes a separate criminal offence, the locally applicable rules of criminal liability shall apply.
- That he or she **shall not be subject to any Retaliatory Action** for reporting or disclosing information in compliance with the Regulations.

Verallia does not tolerate any form of retaliation, threats or attempts to use such measures against Whistleblowers, such as harassment.
The Facilitators as well as the Persons connected with the Whistleblower and the legal entities controlled by the Whistleblower or for which he or she works, are included in Verallia's non-retaliation policy and benefit from the same protections as the Whistleblower.
Disciplinary proceedings or civil or criminal sanctions may be taken against the perpetrator of such retaliation or against any person who does not respect the Whistleblower's rights.

[7]Under French law, pursuant to Article 122-9 of the Penal Code, "A person who breaches a secret protected by law shall not be criminally liable, provided that such disclosure is necessary and proportionate to the safeguarding of the interests in question, that it is made in compliance with the conditions for reporting defined by law and that the person meets the criteria for the definition of a whistleblower set out in Article 6 of Law No. 2016-1691 of December 9, 2016 on transparency, combating corruption and modernizing economic life.
Nor shall a whistleblower be criminally liable if he or she removes, misappropriates or conceals the documents or any other material containing the information of which he or she has lawfully become aware and which he or she reports or discloses under the conditions mentioned in the first paragraph of this article.
The present article is also applicable to the accomplice of these offences.

3.3 Confidentiality

The Processing of the Alert is carried out while respecting **integrity and confidentiality** of the information collected in the Alert, notably the identity of the Whistleblower, as well as that of the persons concerned by the Alert and of any third parties mentioned therein in accordance with the applicable law.

In this respect:

- The persons designated to handle Alerts are the persons mentioned in article 2.6.2 and 3.4.1 of this document. Access to the information collected in the framework of the Alert is forbidden to any person not authorized to know it.
- All persons involved in the management of Alerts are specially trained and bound by a reinforced obligation of confidentiality. In particular, they undertake not to use the data for improper purposes and to respect the limited period of retention of data in accordance with the applicable law.
- The Whistleblower is encouraged to identify himself, but his identity is treated confidentially by the organization in charge of managing the Alerts.
- Identifying information may only be disclosed with the Whistleblower's consent[8].
- The elements likely to identify the person involved in an alert shall not be disclosed, except to the judicial authority, once it has been established that the alert is well founded.

Within the limits of their attributions, the persons in charge of the Platform can also access the data for the purposes of administration of the Platform.

3.4 Protection of personal data

3.4.1 Personal Data

- The Whisteblowing Alert System is implemented by Verallia SA within the Group in order to meet its legal obligations and in the legitimate interest of Verallia to conduct its business with integrity and ethics with regard to matters covered by the Code of Ethics.
- Categories of data processed via the Whistleblowing Platform: Verallia is committed to only process data which is adequate, relevant, and not excessive in relation to the objectives for which it is being collected. Only the following categories of data can be processed:
  - Identity, functions and contact information of the Whistleblower;
  - Identity, functions and contact information of the persons subject to and/or mentioned in an Alert;
  - Identity, functions and contact information of the persons involved in the reception or treatment of the Alert;
  - The facts that are being reported;
  - Elements of information collected during the verification of the reported fact;
  - Summary report of the verification processes;

[8] They may, however, be communicated to the judicial authorities, in the event that the persons responsible for collecting or processing the Alerts are required to report the facts to the judicial authorities (for example: sexual assault or abuse inflicted on (i) a minor or (ii) a vulnerable person (due to illness, infirmity, physical or mental deficiency, or pregnancy)). The whistleblower is then informed, unless such information would jeopardize the legal proceedings. Written explanations are attached to this information.

- Follow-up actions related to the Alert.

- **Recipients**: In addition to the persons authorised to process the data as part of their assignment, Verallia S.A. may communicate data:
  - To the group entity to which the facts relate and/or to any internal and/or external experts (human resources department, internal audit director, lawyers, chartered accountant, analysts, etc.) that Verallia may call on to process the Alert.
  - To the service provider(s) responsible for supplying and operating the Platform and the Phone Line.

  Where applicable, data may be sent to the judicial authority, it being specified that:
  - Any elements that may identify the Whistleblower can only be disclosed to the judicial authorities with the consent of the Whistleblower[9];
  - Any elements that may identify the person involved in an Alert can only be disclosed once it has been established that the Alert is founded.

- **Protection measures for personal data:** Verallia S.A. takes all necessary precautions to preserve the security of the data both when it is collected and when it is communicated or stored. In this context, the data processing can only be accessed via the Platform with a user identification and an individual password that are regularly renewed, or by any other authentication method. These logins are recorded and their frequency is controlled.

3.4.2 Retention of personal data

Within the framework of the Whistleblowing System:

- The recordings, transcripts and documents are kept for the time necessary to process the alert and to protect their authors, the persons they refer to and the third parties they mention, in accordance with the applicable regulations and Verallia's rules and procedures regarding protection and storage.
- In this context, personal data is stored in the following manner:
  - When an Alert is considered not to fall within the areas described in section 2.2 "What alerts to report", the Alert is closed and the data concerning it is anonymized without delay;
  - When no action is taken on an Alert, the data is anonymized after the closure of the verifications according to the laws and regulations in force;
  - When action is taken on the alert (i.e., any decision taken by Verallia to draw consequences from the alert, such as an internal action plan, adoption or modification of internal rules, reorganization of operations or services, pronouncement of a sanction, implementation of legal action, etc.), the data relating to the alert is kept until the end of the procedure and/or until the statute of limitations has expired or all avenues of recourse have been exhausted
  - The data may be kept longer, in archiving involving restricted access, if Verallia is legally obliged to do so (for example, to meet accounting, social or tax obligations).

[9] Except as provided in footnote 8 above.

3.4.3 Transfer of the Data outside of the European Union

For the purpose of treating the Alert, Personal data are hosted in the Platform in Europe. Nevertheless, they can be transferred (i) by Verallia to other entities of the Verallia Group or third parties registered in countries within or outside of the European Economic Area (EEA) for the purpose of handling the Alert or (ii) by the provider of the Platform and of the Phone Line for support and maintenance needs. This includes countries which do not have the same level of protection of personal data as in the EEA.

Verallia ensures that such transfers are carried out by Verallia in compliance with applicable personal data protection regulation and will be secured through adequate data privacy safeguards such as the conclusion of standard contractual clauses adopted by the EU Commission.

Additional information regarding transfers outside the EEA is available to individuals upon request (to donnees.personnelles@verallia.com).

3.4.4 Rights of individuals

The Whistleblowing System guarantees the confidentiality and the respect of the rights throughout the treatment of Alerts.

The recipient informs the Whistleblower upon reception of the Alert according to the Procedure. Accordingly, the person subject to an Alert is informed that his/her personal data is being registered (electronically or not). This information is delivered within one month following the issuing of the Alert, unless it is likely to make impossible or to seriously compromise the purposes of the processing (for example, risk of destruction of evidence relating to the Alert). In this case, the person subject to an Alert is only informed when the risk is eliminated.

Any person identified in this Whistleblowing System, whether the Whistleblower or a person subject to an Alert, has the right to access his/her personal data. Any identified person may also request the rectification or erasure of their data under the conditions and limits provided for by the applicable regulations. He/she may also object to the processing (provided that this right is applicable) or request its limitation.

With regard to the rights of rectification and erasure, these may not allow the retroactive modification of the elements contained in an alert or collected during its investigation. These rights may only be exercised to rectify factual data whose material accuracy can be verified by Verallia S.A. with evidence and without erasing or replacing the data, even if erroneous, initially collected.

These rights may be exercised at the following address: donnees.personnelles@verallia.com .

It should however be noted that the person subject to an Alert can under no circumstances obtain information regarding the identity of the Whistleblower, based on the right to access personal data.

If, after contacting Verallia, the data subject considers that their rights are not respected or that the processing does not comply with the data protection rules, they may lodge a complaint to the competent supervisory authority (the French Data Protection Authority (CNIL) for France).

4 Reporting to the Compliance Committee

The Group Compliance Officer reports to the Compliance Committee once a year about Alerts, management, and the actions taken in this context. This information shall be limited to that which is strictly necessary and proportional to the purpose of the communication.

5 Contacts

Entity: Verallia S.A.
Postal address: Tour Carpe Diem, 31 Place des Corolles, 92400 Courbevoie, France
For the attention of the Group Compliance Officer.
E-mail address: compliance@verallia.com

March 2023

Issued by the Group CSR & Legal Director Wendy Kool-Foulon _____

wendy kool-foulon (22 mars 2023 10:25 GMT+1)

Approved by the CEO Patrice Lucas_____

Patrice Lucas

Patrice Lucas (22 mars 2023 17:13 GMT+1)

APPENDIX: LIST OF NATIONAL EXTERNAL AUTHORITIES

1. FRANCE

1.1. 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 ;

1.2. Services, produits et marchés financiers et prévention du blanchiment de capitaux et du financement du terrorisme :

- Autorité des marchés financiers (AMF), pour les prestataires en services d'investissement et infrastructures de marchés ;
- Autorité de contrôle prudentiel et de résolution (ACPR), pour les établissements de crédit et organismes d'assurance ;

1.3. Sécurité et conformité des produits :

- Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF);
- Service central des armes et explosifs (SCAE) ;

1.4. Sécurité des transports :

- Direction générale de l'aviation civile (DGAC), pour la sécurité des transports aériens ;
- Bureau d'enquêtes sur les accidents de transport terrestre (BEA-TT), pour la sécurité des transports terrestres (route et fer) ;
- Direction générale des affaires maritimes, de la pêche et de l'aquaculture (DGAMPA), pour la sécurité des transports maritimes ;

1.5. Protection de l'environnement :

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

1.6. Radioprotection et sûreté nucléaire :

- Autorité de sûreté nucléaire (ASN) ;

1.7. Sécurité des aliments :

- Conseil général de l'alimentation, de l'agriculture et des espaces ruraux (CGAAER);
  Agence nationale chargée de la sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES) ;

1.8. Santé publique :

- Agence nationale chargée de la sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES) ;
- Agence nationale de santé publique (Santé publique France, SpF) ;
- Haute Autorité de santé (HAS) ;

- Agence de la biomédecine ;
- Etablissement français du sang (EFS) ;
- Comité d'indemnisation des victimes des essais nucléaires (CIVEN) ;
- Inspection générale des affaires sociales (IGAS) ;
- Institut national de la santé et de la recherche médicale (INSERM) ;
- Conseil national de l'ordre des médecins, pour l'exercice de la profession de médecin ;
- Conseil national de l'ordre des masseurs-kinésithérapeutes, pour l'exercice de la profession de masseur- kinésithérapeute ;
- Conseil national de l'ordre des sages-femmes, pour l'exercice de la profession de sage-femme ;
- Conseil national de l'ordre des pharmaciens, pour l'exercice de la profession de pharmacien ;
- Conseil national de l'ordre des infirmiers, pour l'exercice de la profession d'infirmier ;
- Conseil national de l'ordre des chirurgiens-dentistes, pour l'exercice de la profession de chirurgien-dentiste ;
- Conseil national de l'ordre des pédicures-podologues, pour l'exercice de la profession de pédicure- podologue ;
- Conseil national de l'ordre des vétérinaires, pour l'exercice de la profession de vétérinaire ;

1.9. Protection des consommateurs :

- Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) ;

1.10. 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) ;

1.11. Violations portant atteinte aux intérêts financiers de l'Union européenne :

- Agence française anticorruption (AFA), pour les atteintes à la probité ;
- Direction générale des finances publiques (DGFIP), pour la fraude à la taxe sur la valeur ajoutée ;
- Direction générale des douanes et droits indirects (DGDDI), pour la fraude aux droits de douane, droits anti- dumping et assimilés ;

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

1.13. Activités conduites par le ministère de la défense :

- Contrôle général des armées (CGA) ;
- Collège des inspecteurs généraux des armées ;

1.14. Statistique publique :

- Autorité de la statistique publique (ASP) ;

1.15. Agriculture :

- Conseil général de l'alimentation, de l'agriculture et des espaces ruraux (CGAAER) ;

1.16. Education nationale et enseignement supérieur :

- Médiateur de l'éducation nationale et de l'enseignement supérieur ;

1.17. Relations individuelles et collectives du travail, conditions de travail :

- Direction générale du travail (DGT)

1.18. Emploi et formation professionnelle :

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

1.19. Culture :

- Conseil national de l'ordre des architectes, pour l'exercice de la profession d'architecte ;
- Conseil des maisons de vente, pour les enchères publiques ;

1.20. 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 ;

1.21. Intérêt supérieur et droits de l'enfant :

- Défenseur des droits ;

1.22. Discriminations :

- Défenseur des droits ;

1.23. Déontologie des personnes exerçant des activités de sécurité :

Défenseur des droits.

Politique Dispositif Alerte professionnelle - Mars 2023 FINAL

Rapport d'audit final 2023-03-22

Créé le :	2023-03-21
De :	Samira El Montassir (samira.elmontassir@verallia.com)
État :	Signés
ID de transaction :	CBJCHBCAABAAdA_uln7SN1CrXFXhHIrXJUCVTi3U4JOK

Historique « Politique Dispositif Alerte professionnelle - Mars 2023 FINAL »

Document créé par Samira El Montassir (samira.elmontassir@verallia.com)
2023-03-21 - 16:10:06 GMT

Document envoyé par courrier électronique à wendy kool-foulon (wendy.kool-foulon@verallia.com) pour signature
2023-03-21 - 16:11:45 GMT

Courrier électronique consulté par wendy kool-foulon (wendy.kool-foulon@verallia.com)
2023-03-22 - 09:25:37 GMT

Document signé électroniquement par wendy kool-foulon (wendy.kool-foulon@verallia.com)
Date de signature : 2023-03-22 - 09:25:52 GMT - Source de l'heure : serveur

Document envoyé par courrier électronique à patrice.lucas@verallia.com pour signature
2023-03-22 - 09:25:53 GMT

Courrier électronique consulté par patrice.lucas@verallia.com
2023-03-22 - 16:12:08 GMT

Le signataire patrice.lucas@verallia.com a saisi ce nom lors de la signature en tant que Patrice Lucas
2023-03-22 - 16:13:01 GMT

Document signé électroniquement par Patrice Lucas (patrice.lucas@verallia.com)
Date de signature : 2023-03-22 - 16:13:03 GMT - Source de l'heure : serveur

Accord terminé
2023-03-22 - 16:13:03 GMT