	Gestion des incidents et alerte éthique	Référence : I.4 Version : 1.2

Responsabilité	
Responsable de la procédure	Pascale BRADBURY
Service	Ensemble des collaborateurs
Correspondant relais	Pascale BRADBURY

Objectif de la procédure
Conformément à la réglementation, LONVIA CAPITAL a mis en place une procédure et un outil permettant à l'ensemble de ses salariés et aux personnes physiques externes de : - Déclarer des violations du droit au travers d'un outil de traitement des alertes afin de garantir l'anonymat de l'informateur - Faire part au responsable du traitement des alertes/RCCI, d'un dysfonctionnement, d'une entrave à la conformité. Au travers du dispositif décrit de centralisation et de traitement des anomalies identifiées, il s'agit pour LONVIA CAPITAL : - D'identifier et d'encadrer les zones de risques ; - D'améliorer les processus et procédures le cas échéant ; - D'alimenter par des cas pratiques, l'évaluation annuelle de certains prestataires.

Liste des outils/applications utilisés	
Outil(s)	Excel ; PDF
Application(s)	Outlook ; integrityLog par Euronext

Liste des états utilisés	Archivage (oui/non)	Emplacement d'archivage
Fiche incident	Oui	
Base incidents	Oui	

Gestion des mises à jour de la procédure				
Version	**Date**	**Statut**	**Auteur des modifications**	**Nature des modifications**
1.0	06/04/2020	A valider	AGAMA CONSEIL	Création
1.1	10/09/2020	Achevé	J-B BARENTON	Modification nom et validation
1.2	23/11/2023	Achevé	P BRADBURY	Intégration des modifications sur le Droit d'alerte , ajout de l'outil IntegrityLog et Annexe pour l'Espagne

	Gestion des incidents et alerte éthique	Référence : I.4 Version : 1.2

Sommaire

1. DEFINITIONS

Un **incident** est un évènement qui survient et modifie le déroulement attendu et normal des choses. Il est la matérialisation d'un risque opérationnel.

Le **risque opérationnel** est défini par le Comité de Bâle comme le « risque de pertes provenant de processus internes inadéquats ou défaillants, de personnes et systèmes ou d'événements externes ». Recouvrent notamment le risque opérationnel :

- Les incidents survenus suite à des erreurs humaines, des fraudes et malveillances ;
- Des défaillances des systèmes d'information ;
- Des problèmes liés à la gestion du personnel ;
- Des litiges commerciaux, des accidents, incendies, inondations.

Un « **traitement de données personnelles** » est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement).

Est aussi considéré comme un incident un évènement qui constitue un risque sérieux de réputation pour LONVIA CAPITAL et qui est causé par la conduite d'un client, d'un employé ou d'un prestataire de services.

Toutefois, les réclamations clients n'entrent pas dans ce périmètre, la réglementation définit précisément les conditions de traitement des réclamations clients/porteurs et LONVIA CAPITAL a mis en place une procédure spécifique encadrant ce dispositif.

Un **dysfonctionnement** est généré par le doute de tout collaborateur quant à la conformité réelle vis-à-vis de la réglementation ou des procédures internes de toute opération ou activité.

L'alerte éthique (ou "*whistleblowing*") est un dispositif mis à la disposition des salariés qui leur permet de signaler des problèmes pouvant sérieusement affecter l'activité d'une entreprise ou engager gravement sa responsabilité.

2. SIGNALEMENT ET TRAITEMENT DES DYSFONCTIONNEMENTS ET INCIDENTS

A. Détection et communication du dysfonctionnement ou incident

Tout collaborateur de LONVIA CAPITAL s'engage à communiquer sans délai au RCCI les incidents constatés, qu'il soit ou non impliqué dans l'évènement ou que l'anomalie soit le fait d'un prestataire ou de la société elle-même.

Le déclarant consigne cette anomalie dans la « fiche de déclaration d'incident opérationnel ou IT »[1] prévue à cet effet, en renseignant tous les champs d'identification de l'anomalie pour lesquels il dispose de l'information.

[1] Annexe 1

La fiche de déclaration d'incident opérationnel ou IT est ensuite adressée au RCCI avec toute la documentation disponible utile à la parfaite compréhension de l'anomalie. Le RRCI dirigeant en fait une première analyse en fonction de la nature et de l'impact réel ou potentiel de l'incident déclaré.

Il est souhaitable que le collaborateur déclarant, propose à la Direction une action corrective, qui une fois validée par le RCCI, est initiée. Il peut également solliciter le RCCI sur la mesure corrective à mettre en œuvre.

B. Traitement de l'anomalie

L'analyse de l'anomalie/l'incident par le RCCI permet d'en établir la typologie. Il peut s'agir d'une erreur ponctuelle interne, une défaillance d'un système d'information, une erreur d'un prestataire, etc. Le RCCI apprécie ainsi le risque opérationnel résultant de la défaillance imputable soit aux procédures, aux systèmes internes ou à des événements extérieurs.

Il prend, le cas échéant, des mesures de façon à éviter que l'anomalie ne se reproduise : renforcement du dispositif, renforcement des contrôles de 1er niveau, modification de la procédure opérationnelle correspondante …

Le RCCI suit et s'implique dans la résolution de l'incident. La régularisation de l'incident et sa clôture sont notifiées dans la fiche incident. La fiche de déclaration d'incident opérationnel ou IT est enfin visée par le RCCI-dirigeant.

Des actions de sensibilisation des collaborateurs peuvent être également engagées par le RCCI, suivant le niveau de risque lié à l'anomalie détectée.

Tous les documents et échanges éventuels relatifs au traitement de l'anomalie sont enregistrés dans un dossier dédié sur le serveur de LONVIA CAPITAL et classés dans un dossier physique.

Tout incident pour lequel LONVIA CAPITAL a appliqué une mesure disciplinaire, à raison de manquements à ses obligations professionnelles, à l'égard d'une personne physique détentrice de la carte de RCCI, doit être notifié à l'Autorité des Marchés Financiers dans un délai d'un mois maximum par le dirigeant de la société.

C. Renseignement de la « base incidents »

Le RCCI renseigne la « Base incidents »[2]. Le RCCI ou son délégataire exploite périodiquement cette base afin de suivre la fréquence des incidents, leurs délais de régularisation, les actions correctrices mises en œuvre, les plans d'amélioration des procédures en place.

Cette « Base incidents » permet également d'appuyer l'évaluation des prestataires réalisée annuellement par LONVIA CAPITAL.

D. Responsabilités des dirigeants et des instances de surveillance

Le Règlement Général de l'AMF a mis en œuvre une règle, pour les sociétés de gestion gérant des OPC, qui implique que les dirigeants effectifs de LONVIA CAPITAL doivent déclarer à l'AMF sans délai :

[2] Annexe 2

- Les incidents dont la survenance est susceptible d'entrainer :
  - Une perte ou un gain ;
  - Un coût lié à la mise en cause de sa responsabilité civile ou pénale ;
  - Un coût lié à une sanction administrative ;
  - Une atteinte à la réputation ;

  Et dont l'incidence excède 5% des Fonds Propres Réglementaires

- Tout évènement ne permettant plus à LONVIA CAPITAL de satisfaire aux conditions de son agrément.

Cette déclaration prend la forme d'un compte rendu d'incident indiquant la nature de l'incident, les mesures adoptées et les initiatives prises pour éviter que l'incident se reproduise.

3. L'ALERTE ETHIQUE

La loi n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte, donne une définition plus large des lanceurs d'alerte, simplifie les canaux de signalement, élargit la protection contre les représailles à l'entourage du lanceur d'alerte

Le décret du 3 octobre 2022 a fixé les modalités selon lesquelles sont établies les procédures internes et externes de recueil et de traitement des signalements.

Conformément aux dispositions de la loi 2/2023 du 20 février réglementant la protection des personnes qui signalent des violations de la réglementation et la lutte contre la corruption, LONVIA CAPITAL, SUCURSAL EN ESPAÑA ("succursale LONVIA") a mis en place un dispositif de signalement interne. (Annexe 4)

A. Remontée interne

Tout collaborateur peut signaler via l'outil IntegrityLog à l'adresse suivante Whistleblower (complylog.com) , sans contrepartie financière directe et de bonne foi, des informations portant :

1. sur un crime ou un délit ;
2. une menace ou un préjudice pour l'intérêt général ;
3. une violation ou une tentative de dissimulation d'une violation :
   - ✓ d'un engagement international régulièrement ratifié ou approuvé par la France ;
   - ✓ 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.

Dans un contexte professionnel, le lanceur d'alerte peut désormais signaler des faits qui lui ont été simplement rapportés ;

Le périmètre de l'alerte éthique ou alerte professionnelle, est rappelé dans le référentiel relatif aux dispositifs d'alertes professionnelles (DAP) de la CNIL. (Annexe 3)

L'informateur peut choisir librement le canal, interne ou externe, auquel adresser sa communication.
Dans le cas du canal interne de LONVIA, vous pouvez décider de soumettre l'information par le biais du canal Whistleblower (complylog.com) qui garantit l'anonymat de l'informateur, ou, si vous le souhaitez, en personne, par courrier électronique, en utilisant le formulaire.

Le lanceur d'alerte est protégé et ne fera pas l'objet de mesures discriminatoires, notamment en matière de licenciement, de rémunération ou de formation. En alertant le responsable du traitement des alertes qui est le RCCI de LONVIA , le lanceur d'alerte n'est pas pour autant exonéré de sa responsabilité si lui-même a enfreint les règles.

La confidentialité des données du lanceur d'alerte est garantie tout au long du processus de gestion des informations transmises.
À cet égard, l'accès aux données à caractère personnel contenues dans la politique d'alerte est limité, dans le cadre de ses pouvoirs et fonctions, exclusivement aux personnes suivantes :
(A) Le gestionnaire du système et toute personne qui le gère directement.
(B) Le directeur des ressources humaines, uniquement lorsque des mesures disciplinaires peuvent être prises à l'encontre d'un employé.
(C) La personne responsable des services juridiques de LONVIA, au cas où il serait nécessaire d'engager une action en justice en rapport avec les faits décrits dans la communication.
(D) Les responsables du traitement des données qui peuvent être désignés de temps à autre.
(E) Le délégué à la protection des données.

Le lanceur d'alerte a le droit de connaître l'état d'avancement du traitement de sa communication et le résultat dans les délais fixés par la loi 2/2023.

La loi 2/2023 établit que le traitement des données personnelles découlant de son application sera régi par les dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (règlement général sur la protection des données, GDPR) ; dans la loi organique 3/2018 du 5 décembre sur la protection des données personnelles et la garantie des droits numériques ; et dans le titre VI de la loi 2/2023 elle-même.
Le gestionnaire du système d'information interne est responsable du traitement des données reçues par le canal d'information interne établi.

Le RCCI de LONVIA CAPITAL enregistre les éléments sur un support durable, consultable par l'AMF.
Depuis le 1er septembre 2022, le lanceur d'alerte dispose de deux canaux de signalement, qu'il choisit librement : un signalement interne et un signalement externe, sans hiérarchie entre ces canaux.

B. Remontée à l'AMF

Le lanceur d'alerte peut donc appliquer la procédure externe sans avoir au préalable recouru à la procédure interne de signalement. De même, une divulgation publique directe est permise dans certains cas.
Par ailleurs, l'AMF s'est doté d'un dispositif lui permettant de recevoir et de traiter les alertes portant sur des potentiels manquements à la réglementation dont elle assure la surveillance et qui garantit la confidentialité de l'auteur de la notification et des personnes visées, en application 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.

L'AMF s'engage à traiter de manière confidentielle toutes alertes qu'elle recevrait par des procédures mises en place en son sein.

Pour signaler un fait dont un collaborateur de LONVIA CAPITAL aurait eu connaissance à l'encontre des textes européens, au code monétaire et financier ou au règlement général de l'AMF, le collaborateur peut contacter l'AMF :

- https://www.amf-france.org/fr/lanceur-dalerte
- Par courrier à :

AMF Direction des affaires juridiques
17 place de la Bourse
75082 Paris Cedex 02
en indiquant la mention « CONFIDENTIEL » sur l'enveloppe (ou en suivant la procédure mentionnée précédemment dans les cas particuliers)

- Par téléphone : 01 53 45 64 44 de 9h à 12h et de 14h à 17h

Par souci de confidentialité, il est recommandé d'utiliser le service personnel de messagerie électronique ou le téléphone personnel du collaborateur plutôt que ceux de LONVIA CAPITAL. L'AMF s'engage à ce que seuls les personnels spécialisés de l'AMF traiteront le dossier et auront accès à l'identité du lanceur d'alerte et de l'auteur désigné, et à effectuer un suivi adapté et attentif du dossier porté à leur attention. L'AMF s'engage à réaliser un suivi régulier de l'alerte, par les seuls personnels spécialisés.

C. Remontée adressée directement au Défenseur des Droits

A noter si le collaborateur connait des doutes sur l'organisme compétent à recevoir et à traiter l'alerte, celle-ci peut être adressée au Défenseur des droits qui l'orientera vers l'organisme approprié.

Urgence justifiant l'absence de saisine de l'organisme en cause dans l'hypothèse où les faits à l'origine de l'alerte paraissent constituer :

- Un danger grave et imminent ;
- Ou un risque de dommages irréversibles.

Le collaborateur pourra porter son signalement directement à la connaissance :

- De l'autorité judiciaire ;
- De l'autorité administrative ;
- De l'ordre professionnel.

Ces instances peuvent être saisies alternativement ou simultanément. Il est préférable d'effectuer cette saisine en recommandé avec accusé de réception.

Il est également recommandé de respecter les modalités de transmission suivantes pour assurer le respect des règles de confidentialité :

- Le signalement devra être adressé par la poste, par écrit et sous double enveloppe.

- Tous les éléments de la saisine doivent être insérés dans une enveloppe fermée – dite enveloppe intérieure - laquelle sera insérée dans une seconde enveloppe adressée au Défenseur des droits, dite enveloppe extérieure.
- Sur l'enveloppe intérieure figurera exclusivement la mention suivante : « SIGNALEMENT D'UNE ALERTE (date de l'envoi) » Sur l'enveloppe extérieure figurera l'adresse d'expédition :

Défenseur des droits Libre réponse
71120 75342 PARIS CEDEX 07
Défenseur des Droits (defenseurdesdroits.fr)

Un accusé réception sera adressé au collaborateur comportant un numéro identifiant qu'il lui appartiendra d'utiliser pour l'ensemble de ses échanges avec le Défenseur des droits.
Si le collaborateur estime que le signalement est d'une particulière gravité, il dispose également de la faculté de rendre publique l'alerte.

Ce dispositif exceptionnel ne doit être utilisé qu'avec un grand discernement car le lanceur d'alerte ne pourra être reconnu irresponsable pénalement que si son appréciation de l'urgence de la situation est incontestable. La divulgation publique ne peut donc être envisagée qu'en dernier ressort en cas d'impossibilité manifeste d'agir autrement pour faire cesser le risque à l'origine de l'alerte.

ANNEXE 1 : FICHE DE DECLARATION D'INCIDENT OPERATIONNEL OU IT

FICHE DE DECLARATION D'INCIDENT OPERATIONNEL OU IT

ZONE RESERVEE AU RCCI

Date réception | Date de clôture | Référence

Commentaire

EXPEDITEUR

Nom, Prénom | Département

IDENTIFICATION DE L'INCIDENT

Date incident | Date détection | PTF concernés

IMPACT FINANCIER

Gain/Perte/Nul | Montant | Devise

Incidence équivalent à ____ %* des Fonds Propres Réglementaires

DESCRIPTION ET TRAITEMENT DE L'INCIDENT

Circonstances

Responsabilités

Mesure(s) de régularisation

Mesure(s) corrective(s) de prévention

**les incidents dont la survenance est susceptible d'entrainer : une perte ou un gain, un coût lié à la mise en cause de sa responsabilité civile ou pénale, un coût lié à une sanction administrative, une atteinte à la réputation, et dont l'incidence excède 5% des Fonds Propres Réglementaires doivent être déclarés à l'AMF sans délai.*

ANNEXE 2 : BASE INCIDENTS

Disponible dans le répertoire procédures.

ANNEXE 3 : REFENTIEL RELATIF AUX DISPOSITIF D'ALERTES PROFESSIONNELLES (DAP)

La mise à jour du référentiel relatif aux dispositifs d'alerte professionnelle en questions | CNIL

ANNEXE 4 : DISPOSITIF DU DROIT D'ALERTE EN ESPAGNE

a. Introduction et contexte

La politique d'Alerte de LONVIA CAPITAL (**" LONVIA** ") contient les principes de base de la gestion des incidents ou des dysfonctionnements pouvant donner lieu à des risques opérationnels pour LONVIA, tels que définis dans la Directive Européenne d'alerte , et définit également la procédure d'alerte, également appelée " alerte éthique " ou " whistleblowing " dans la Directive Européenne d'alerte.

La présente annexe (" **Annexe WB espagnole** " ou l'" **Annexe** ") contient les particularités applicables à de LONVIA CAPITAL, SUCURSAL EN ESPAÑA (" **Branche LONVIA** ") , conformément à la loi 2/2023 du 20 février, réglementant la protection des personnes qui signalent des infractions réglementaires et la lutte contre la corruption (**" Loi 2/2023 "**) et transposant en Espagne la directive 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 (" **Directive WB** ").

La mise en œuvre en Espagne de la **"politique d'alerte**", qui se compose de la politique **d'alerte de LONVIA Capital (pour le bureau de Paris)** et de l'annexe espagnole **d'alerte, a été** approuvée par le conseil d'administration de LONVIA Capital, sans consultation préalable des représentants des travailleurs, étant donné qu'il n'existe pas d'organe de ce type en Espagne.

Pour tout ce qui ne figure pas dans la présente annexe, y compris la procédure à suivre en cas de réception d'informations, c'est la politique de droit d'alerte de LONVIA CAPITAL qui s'applique.

b. Canal d'information interne à la branche LONVIA et canaux externes

Le canal d'information interne de la branche LONVIA est Whistleblower (complylog.com) il est le canal privilégié pour signaler les actions ou omissions visées à l'article 2 de la loi 2/2023, comme indiqué dans la section 4 de ce document, qui peut être consulté via le lien suivant :

Whistleblower (complylog.com)

Par l'intermédiaire de l'outil COMPLYLOG, les personnes énumérées dans la présente annexe peuvent signaler tout manquement à la loi, aux politiques internes ou au code de conduite de LONVIA, comme indiqué dans la présente politique d'alerte.

De même, la personne déclarante (telle que définie dans la présente politique) peut demander à rencontrer le responsable du système interne de l'agence LONVIA, la réunion ayant lieu dans les 7 jours suivant la demande de la personne déclarante. La réunion sera enregistrée pour lequel une nouvelle procédure sera lancée au début de la réunion.

En outre, les personnes protégées par la politique d'alerte peuvent s'adresser au canal externe établi par l'autorité indépendante de protection des dénonciateurs (à créer) ou les autorités équivalentes au niveau régional (pour le signalement d'infractions liées à la législation régionale).

En effet, pour obtenir des informations sur d'éventuelles infractions relevant des administrations publiques des communautés autonomes et des villes autonomes espagnoles :

- Canal del Informante de la Comunidad de Madrid
- Office de lutte contre la fraude de Catalogne
- Agence valencienne de lutte contre la fraude
- Office andalou de lutte antifraude
- Office de prévention et de lutte contre la corruption des îles Baléares

Pour la notification d'éventuelles infractions dans le domaine des marchés de valeurs mobilières : CNMV - Notification d'éventuelles infractions dans le domaine des marchés de valeurs mobilières.

Pour le signalement d'éventuelles infractions liées au blanchiment de capitaux et à la lutte contre le terrorisme : SEPBLAC, l'unité espagnole de renseignement financier intégrée à la Banque d'Espagne.

En outre, LONVIA, dans le cadre de sa politique d''alerte, a mis à la disposition de tous les membres de son organisation d'autres canaux d'information définis dans cette politique. Dans ce cas, le dénonciateur sera soumis aux procédures décrites dans cette politique[3] .

c. Responsable du traitement des alertes Internes

Conformément aux dispositions de la loi 2/2023, une personne physique a été nommée responsable du système d'information interne et exerce ses fonctions de manière autonome et indépendante.

Le conseil d'administration de la LONVIA est chargé de nommer le responsable du système d'information interne de la branche LONVIA et de notifier l'autorité indépendante de protection des lanceurs d'alerte (une entité en cours de création).Le conseil d'administration de LONVIA a actuellement nommé un responsable du système d'information interne :

PASCALE BRADBURY
9 avenue de l'Opéra, 75001 Paris

[3] Saisine du MAE et saisine directe du Défenseur des droits

d. Champ d'application matériel de la politique de d'alerte

La politique de d'alerte et la protection qu'elle offre s'appliquent aux personnes qui signalent les violations suivantes :

Tout acte ou omission pouvant constituer une infraction à la législation de l'Union européenne à tout moment, conformément à l'article 2 de la loi 2/2023.

Entrer dans le champ d'application des actes de l'Union européenne énumérés à l'annexe de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 relative à la protection des personnes signalant des violations du droit de l'Union, indépendamment de leur qualification en droit national ;

affectent les intérêts financiers de l'Union européenne tels que visés à l'article 325 du traité sur le fonctionnement de l'Union européenne (TFUE) ; ou

ont une incidence sur le marché intérieur, tel que visé à l'article 26, paragraphe 2, du TFUE, y compris les infractions aux règles de concurrence de l'UE et les aides accordées par les États, ainsi que les infractions relatives au marché intérieur en ce qui concerne les actes contraires aux règles de l'impôt sur les sociétés ou les pratiques visant à obtenir un avantage fiscal qui irait à l'encontre de l'objet ou du but de la législation applicable à l'impôt sur les sociétés.

Actions ou omissions pouvant constituer une infraction pénale ou administrative grave ou très grave. En tout état de cause, il faut entendre par là toutes les infractions pénales ou administratives graves ou très graves qui entraînent un préjudice financier pour le Trésor public et la sécurité sociale.

Ceci sans préjudice de certaines limitations prévues par la loi 2/2023 (voir article 2).

Elle s'applique également aux personnes qui font des rapports sur les sujets énumérés dans la politique d'alerte de LONVIA CAPITAL.

e. Champ d'application de la politique d'alerte

La politique d'alerte s'applique aux personnes suivantes, appelées dénonciateurs /lanceurs d'alerte:

Les employés de la branche LONVIA en Espagne et de LONVIA en France, dans ce dernier cas, pour les questions relatives à la branche LONVIA.

Les travailleurs indépendants qui fournissent des services à la branche LONVIA.

Les actionnaires et les membres du conseil d'administration de LONVIA, pour les questions relatives à la branche LONVIA.

Toute personne travaillant pour des contractants, des sous-traitants ou des fournisseurs de la branche LONVIA ou sous leur supervision et leur direction.

Les personnes qui ont été employées par la branche LONVIA, les bénévoles, les stagiaires, les stagiaires en formation et les personnes dont la relation de travail n'a pas encore commencé dans les cas où des informations sur les infractions ont été obtenues au cours de la procédure de sélection ou de la négociation précontractuelle.

Les personnes qui assistent le dénonciateur dans le processus de signalement et qui peuvent faire l'objet de représailles.

Les personnes liées à l'informateur et susceptibles de subir des représailles, telles que les collègues de travail ou les parents de l'informateur.

Les personnes morales pour lesquelles le répondant travaille ou avec lesquelles il entretient tout autre type de relation dans le cadre d'un emploi ou dans lesquelles il détient une participation significative.

f. Droits des lanceurs d'alerte

L'informateur peut choisir librement le canal, interne ou externe, auquel adresser sa communication.

Dans le cas du canal interne de la branche LONVIA, vous pouvez décider de soumettre l'information par le biais du canal Whistleblower (complylog.com) qui, si vous le souhaitez, garantit l'anonymat de l'informateur, ou, si vous le souhaitez, en personne, par courrier électronique, en écrivant au responsable du traitement des Alertes Ethiques nommé ci dessus.

La confidentialité des données de l'informateur est garantie tout au long du processus de gestion des informations transmises.

À cet égard, l'accès aux données à caractère personnel contenues dans la politique d'alerte est limité, dans le cadre de ses pouvoirs et fonctions, exclusivement aux personnes suivantes :

Le gestionnaire du système et toute personne qui le gère directement.

Le directeur des ressources humaines, uniquement lorsque des mesures disciplinaires peuvent être prises à l'encontre d'un employé.

La personne responsable des services juridiques de LONVIA, au cas où il serait nécessaire d'engager une action en justice en rapport avec les faits décrits dans la communication.

Les responsables du traitement des données qui peuvent être désignés de temps à autre.

Le délégué à la protection des données.

L'informateur a le droit de connaître l'état d'avancement du traitement de sa communication et le résultat dans les délais fixés par la loi 2/2023.

g. Protection des données

La loi 2/2023 établit que le traitement des données personnelles découlant de son application sera régi par les dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (règlement général sur la protection des données, GDPR) ; dans la loi organique 3/2018 du 5 décembre sur la protection des données personnelles et la garantie des droits numériques ; et dans le titre VI de la loi 2/2023 elle-même.

Le gestionnaire du système d'information interne est responsable du traitement des données reçues par le canal d'information interne établi.

h. Personnes concernées

Conformément à la loi 2/2023, pendant le traitement du dossier, les personnes concernées par la communication ont droit à la présomption d'innocence, au droit à la défense et au droit d'accès au dossier prévu par ladite loi, ainsi qu'à la même protection que celle établie pour les informateurs, en préservant leur identité et en garantissant la confidentialité des faits et des données de la procédure.

i. Fausses communications

La loi 2/2023 précise à l'article 63 que le fait de communiquer ou de divulguer publiquement des informations en sachant qu'elles sont fausses constitue un délit très grave.

j. Gestion de l'information : Procédure

Comment rapporter

Comme indiqué dans la procédure du dispositif d'Alerte de LONVIA CAPITAL, les événements entrant dans le champ d'application peuvent être signalés par les canaux qui y sont indiqués, bien que pour les événements survenant dans le champ d'application de la branche LONVIA, conformément à la loi 2/2023, le canal Whistleblower (complylog.com) a été mis à la disposition de la branche LONVIA. b ci-dessus.

Par ailleurs, toute personne ayant connaissance d'une plainte ou d'une information faite en dehors du Whistleblower (complylog.com) doit immédiatement en informer le responsable du système d'information interne de la branche LONVIA, par l'intermédiaire du Canal interne Whistleblower (complylog.com), en maintenant la plus grande confidentialité sur les informations reçues. Le non-respect de cette obligation

de confidentialité peut avoir des conséquences graves pour l'informateur et pour la LONVIA, et fera l'objet d'une procédure disciplinaire pour faute très grave.

Les caractéristiques du canal d'information interne et les principes qui régissent son fonctionnement sont les suivants :

- Garantie de la confidentialité de l'identité de l'informateur dans les communications par le canal interne et tout au long du processus de gestion de l'information.
- Prévoir la possibilité de maintenir la communication avec l'informateur et, si cela est jugé nécessaire, de lui demander des informations supplémentaires.
- Possibilité de soumettre des propositions anonymes.
- Établissement du droit de la personne concernée d'être informée des actes ou omissions qui lui sont imputés et d'être entendue à tout moment.
- Exiger le respect de la présomption d'innocence et de l'honneur des personnes concernées.
- Respect des dispositions relatives à la protection des données personnelles conformément aux dispositions de la loi 2/2023.
- Transmission immédiate de l'information au ministère public lorsque les faits peuvent être révélateurs d'une infraction pénale.

1. Gestion de l'information

- **Réception des informations et évaluation préliminaire**

Les informations sont reçues par le gestionnaire du système d'information interne. (ci-après, le cas échéant, le **" Receveur** ").

Le destinataire accuse réception du rapport à la partie déclarante dans les sept jours suivant sa réception.

Dans le cas de l'application informatique, cet accusé de réception est automatique et prend la forme d'un numéro d'enregistrement/mot de passe qui est utilisé par l'informateur pour suivre la procédure correspondante et, le cas échéant, pour recevoir des communications du destinataire ou pour fournir de nouvelles informations.

Le bénéficiaire fait rapport au RCCI et, à titre d'information, au responsable mondial de la conformité.

Le RCCI, avec le soutien du gestionnaire du système d'information interne, sera responsable du triage de toutes les informations reçues.

À cet égard, le rapport fera l'objet d'un examen préliminaire qui permettra de vérifier :

- l'intégrité ;

- le respect des critères et des exigences énoncés dans la politique d'alerte ;

- l'existence des conditions juridiques et/ou factuelles pour le lancement de la phase d'analyse ultérieure ;

- la gravité éventuelle des faits allégués et l'urgence.

Une fois le contrôle préalable effectué :

- si les informations reçues ne relèvent pas du champ d'application matériel de la politique d'alerte ou ne sont pas conformes aux exigences indiquées dans la politique d'alerte, le destinataire ou la personne chargée du contrôle préalable procède au classement en informant le déclarant (par le canal Whistleblower (complylog.com)) Les raisons de ne pas poursuivre l'analyse doivent être bien documentées et justifiées ;

- si les informations sont trop générales ou incomplètes, le destinataire ou la personne chargée du contrôle préalable prend contact avec le rapporteur par l'intermédiaire des voies de saisine pour demander des éléments supplémentaires utiles à l'évaluation préliminaire ;

- si le destinataire ou la personne chargée de la vérification préalable estime que l'information relève du champ d'application matériel, il/elle passe à la phase d'analyse ultérieure en informant le responsable du traitement par l'intermédiaire du canal ;

Cette phase doit être achevée dans un délai de 10 jours ouvrables à compter de la réception de l'information (ce délai peut être prolongé jusqu'à 15 jours ouvrables si des enquêtes préliminaires sont nécessaires).

À l'issue de la phase préliminaire, le RCCI, en collaboration avec le responsable du système d'information interne et en faisant appel aux ressources internes ou externes jugées nécessaires, établit un rapport (le **"rapport préliminaire")** indiquant le type d'informations, la date de réception, la date d'achèvement de l'évaluation préliminaire et le résultat de l'évaluation préliminaire (archivage ou poursuite de l'analyse), ainsi que les motifs de l'évaluation préliminaire.

2. Analyse des rapports

Si, à la suite de la vérification préliminaire, une enquête est nécessaire, le RCCI peut déléguer l'exécution de l'enquête aux ressources humaines, à la conformité locale, à l'équipe de sécurité des systèmes ou à un tiers spécialisé en la matière, et effectuer, avec le responsable du système d'information interne, une supervision de cette enquête (sauf si les faits concernent le responsable du système d'information interne, auquel cas il ne participera pas à l'enquête).

À ce stade, en veillant à ne pas révéler l'identité de la personne déclarante, des sujets concernés par les informations et de l'objet des informations, la personne chargée de la phase d'analyse et d'évaluation peut (i) interagir avec les autres fonctions et domaines de l'entreprise pour demander leur collaboration, en fournissant des

données, des documents ou des informations utiles à l'analyse elle-même ; (ii) demander des éléments ou des perceptions supplémentaires à la personne déclarante, en enregistrant l'entretien correspondant ; ou (iii) demander l'avis de tiers spécialistes du sujet spécifique sur lequel les informations sont basées.

Le responsable de la phase d'analyse et d'évaluation effectue toute activité jugée utile ou nécessaire, y compris l'audition de l'informateur et/ou de toute autre personne susceptible de fournir des informations sur les faits rapportés, dans le respect des principes de confidentialité et d'impartialité du jugement, de la législation sur la protection des données à caractère personnel et des contrats de travail correspondants applicables.

La personne concernée par l'information a le droit d'être informée des actes ou omissions qui lui sont reprochés et d'être entendue à tout moment. Cette communication a lieu au moment et de la manière jugés appropriés pour assurer le bon déroulement de l'enquête.

L'ensemble de ce processus est réalisé sous la supervision du responsable du système d'information interne.

3. Résultat de l'analyse et rapport final

À l'issue de la phase d'analyse, le RCCI, en collaboration avec le responsable du système d'information interne, qu'il ait ou non délégué l'exécution de l'enquête à un autre service ou domaine de l'entité ou à un tiers spécialisé dans le domaine, établit un rapport final ("**rapport final**"), qui présente les éléments suivants

- les détails de l'information (nom de l'informateur - s'il y a consentement de l'informateur - et de la (des) personne(s) dénoncée(s), lieu et date des faits, preuves ou documentation) ;

- les contrôles effectués, leurs résultats et l'entreprise ou les tiers impliqués dans la phase d'analyse ;

- une évaluation sommaire du processus d'analyse avec une indication des cas trouvés et de leurs raisons ;

- le résultat et la conclusion de l'analyse (archivage ou justification du rapport).

Le rapport final sera envoyé à l'organe de gestion de la branche LONVIA par le responsable du système d'information interne et sera également porté à l'attention de l'organe compétent de la LONVIA par le RCCI.

4. Mesures de prise de décision

Le délai maximal de réponse à la demande de renseignements ne peut excéder trois mois à compter de la réception des informations, sauf dans les cas d'une complexité particulière nécessitant une prolongation du délai, auquel cas celui-ci peut être prolongé d'un maximum de trois mois supplémentaires.

Dès réception du rapport final, c'est le directeur général avec l'avis du responsable du système d'information interne et du RCCI et de la personne chargée de l'enquête interne, qui décide s'il y a lieu d'engager une procédure disciplinaire à l'encontre de la personne responsable de l'infraction ou du comportement illicite et tenue pour responsable à la suite de l'analyse effectuée et de l'évaluation réalisée.

Le responsable du système d'information interne doit informer le ministère public si ces faits sont considérés comme étant de nature criminelle ou transmettre l'information à une autre autorité ou à un autre organe qui pourrait être compétent pour traiter la communication.

Si les faits portent atteinte aux intérêts financiers de l'Union européenne, l'information est transmise au Parquet européen.

5. Interdiction de représailles

Les actes constituant des représailles, y compris les menaces de représailles et les tentatives de représailles à l'encontre des personnes qui soumettent une communication ou une information par le biais du canal Whistleblower (complylog.com)ou par tout autre moyen interne, ou à l'Autorité indépendante de protection des dénonciateurs ou aux autorités équivalentes des Communautés autonomes, ou qui font une divulgation publique conformément aux critères et aux exigences de la loi 2/2023, sont strictement interdits.

Aux fins de la politique d'alerte, on entend par représailles tout acte ou omission interdit par la loi, ou qui implique directement ou indirectement un traitement défavorable qui place les personnes qui le subissent dans une situation de désavantage particulier par rapport à d'autres dans le contexte de l'emploi ou de la profession, uniquement en raison de leur statut de dénonciateur ou parce qu'elles ont fait une divulgation publique.

Les représailles comprennent, sans s'y limiter, les représailles sous forme de :

La suspension du contrat de travail, le licenciement ou la cessation de la relation de travail, y compris le non-renouvellement ou la résiliation anticipée d'un contrat de travail temporaire après la période d'essai, ou la résiliation anticipée ou l'annulation de contrats de biens ou de services, l'imposition de toute mesure disciplinaire, la rétrogradation ou le refus de promotion et toute autre modification substantielle des conditions de travail et la non-transformation d'un contrat de travail temporaire en contrat permanent, dans le cas où l'employé avait des attentes légitimes de se voir offrir un emploi permanent ; à moins que ces mesures n'aient été prises dans le cadre de l'exercice normal des pouvoirs de gestion prévus par la législation du travail, en raison de circonstances, de faits ou d'infractions avérées, et sans rapport avec la présentation de la communication.

Les dommages, y compris les atteintes à la réputation, ou les pertes économiques, la coercition, l'intimidation, le harcèlement ou l'ostracisme.

Évaluation ou références négatives concernant le travail ou les performances professionnelles.

L'établissement d'une liste noire ou la diffusion d'informations dans un domaine sectoriel particulier, qui entrave ou empêche l'accès à l'emploi ou la passation de marchés de travaux ou de services.

Refus ou retrait d'une licence ou d'un permis.

Refus de formation.

Discrimination ou traitement défavorable ou injuste.

6. Archivage de la documentation et des rapports

La branche de la LONVIA tient un registre des informations reçues et des enquêtes internes auxquelles elles donnent lieu, en garantissant, dans tous les cas, les exigences de confidentialité prévues par la loi.

Chaque rapport contient les informations suivantes :

- Date du rapport
- Date de l'événement
- Description
- Situation
- Résolution, si elle est close
- Autres informations sur le récepteur

Toute la documentation relative à la présente procédure est conservée par le responsable interne du système d'information ou la personne désignée par lui pendant une période de 5 ans ou, en tout état de cause, pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elle a été traitée, d'une manière propre à en assurer la confidentialité.

Chaque année, le responsable du système d'information interne ou son représentant prépare un rapport de synthèse sur les rapports reçus, les analyses effectuées et le résultat de ces analyses.

Le rapport peut contenir : (i) une indication de tous les rapports reçus, de ceux qui sont en cours d'analyse et de leur résultat (archivage, évaluation approfondie) ; (ii) l'évaluation des rapports acceptés et leur résultat (archivage, ouverture d'une procédure disciplinaire, sanctions appliquées) ; et (iii) la proposition de critères correctifs ou complémentaires pour la procédure.

Le registre indiqué n'est pas public et n'est accessible que sur demande motivée de l'autorité judiciaire compétente, par ordonnance, dans le cadre d'une procédure judiciaire et sous la tutelle de cette autorité.

7. Infractions

L'Autorité indépendante pour la protection des dénonciateurs est l'organe compétent pour traiter les infractions visées au titre IX de la loi 2/2023 commises dans le secteur public de l'État.

Ces infractions comprennent, entre autres, l'adoption de mesures de rétorsion à l'encontre des dénonciateurs, la violation des garanties de confidentialité et d'anonymat prévues par la loi 2/2023 ou de l'obligation de garder le secret sur tout aspect lié à l'information, ainsi que la communication ou la divulgation publique d'informations en sachant qu'elles sont fausses.