

Dispositif d'alerte Groupe

Champ d'application du dispositif d'alerte Professionnelle

Conformément aux dispositions des articles 8 et 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, dite « Loi Sapin II », et à la loi « Devoir de Vigilance » du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre, le **Groupe met en place un dispositif d'alerte professionnelle (« le Dispositif »)**.

Le dispositif mis en place au sein d'Editis permet aux **Collaborateurs** (en CDI, CDD, stagiaire, intérimaire, salarié d'un prestataire de service) d'émettre, de manière désintéressée et de bonne foi, tout signalement sur des faits dont ils ont eu personnellement connaissance et correspondant aux manquements suivants :

- **Manquements relatifs à la violation du code de conduite anticorruption (article 17-2 de la loi dite « Loi Sapin II »)**
 - L'existence de conduites ou de situations contraires au code de conduite anticorruption d'Editis, dans la mesure où celles-ci sont susceptibles de caractériser des faits de corruption ou de trafic d'influence.

- **Autres manquements (article 6-1 de la loi dite « Loi Sapin II »)**
 - Un crime ou un délit ;
 - Une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France ;
 - Une violation grave et manifeste d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un engagement international régulièrement ratifié ;
 - Une violation grave et manifeste de la loi ou du règlement ;
 - Une menace ou un préjudice grave pour l'intérêt général, dont l'émetteur de l'alerte a eu personnellement connaissance.

- **Atteinte grave envers les droits humains et les libertés fondamentales, la santé et la sécurité des personnes ainsi que l'environnement (article 1 de la loi relative au devoir de vigilance »)**



Toutefois, sont exclues du champ d'application les alertes portant sur des faits couverts par le secret de la défense nationale, par le secret médical et par le secret des relations entre un avocat et son client (article 6-2 de la loi dite « Loi Sapin II »).

Comment faire un signalement dans le dispositif d'alerte ?

Pour effectuer un signalement dans le dispositif d'alerte, **connectez-vous à la plateforme : alerte.vivendi.com**

Une plateforme interne mise à disposition par le Groupe permet aux collaborateurs **agissant de manière désintéressée, de bonne foi, et ayant eu personnellement connaissance des faits entrant dans le champs d'application du dispositif** d'adresser leur signalement.

Une page d'accueil pédagogique est mise à disposition avec notamment des questions-réponses sur les modalités de recevabilité et de traitement du signalement et un renvoi vers une page d'aide à la décision.

Lors du dépôt de l'alerte sur la plateforme, le lanceur d'alerte doit :

- Saisir les informations relatives à son identité (sauf anonymat).
- Joindre à son alerte tout document ou information de nature à prouver les faits allégués.
- Communiquer toutes les données nécessaires et complémentaires demandées par la Cellule d'Orientation et de Traitement des Alertes (COTA).

Une fois l'alerte enregistrée dans la plateforme, le lanceur d'alerte recevra un identifiant et un mot de passe afin de se connecter à son dossier pour suivre le traitement de son alerte, par un changement de statut :

Statut	Définition
En attente de qualification	Le signalement a bien été enregistré sur la plateforme et doit être examiné par la Cellule d'Orientation et de Traitement des Alertes (COTA).
En cours de traitement	Le signalement a été qualifié de recevable et est en cours de traitement par la Cellule d'Orientation et de Traitement des Alertes (COTA).
Clôturé	Le dossier relatif au signalement a été clôturé, soit en raison de l'irrecevabilité de l'alerte, soit en raison de la clôture de l'enquête.

Une adresse de courrier électronique est associée à la plateforme du dispositif d'alerte : alerte@vivendi.com.

Cette adresse a uniquement pour but de permettre au lanceur d'alerte d'échanger sur le fonctionnement de la plateforme (par exemple, la perte d'identifiant et/ou mot de passe) ainsi que demander l'accès, la rectification ou la suppression des données le concernant.

Les destinataires de cette adresse électronique ont pour rôle l'administration du site (Webmaster), et n'auront pas accès aux signalements enregistrés ni aux informations relatives au traitement de ces derniers.

Modalités du dispositif d'alerte

1. Le lanceur d'alerte

Sont visés au titre de lanceur d'alerte tous **les membres du personnel**, d'une part **les collaborateurs internes** (désigne toute personne titulaire d'un contrat de travail), d'autre part **les collaborateurs extérieurs et occasionnels** (désigne toute personne intervenant en mission dans les locaux des entités d'Editis).

L'octroi du statut de lanceur d'alerte est subordonné à quatre conditions cumulatives (**issues de l'article 6 de la loi dite « Loi Sapin II »**) :

- Le lanceur d'alerte doit être une **personne physique** ;
- Le lanceur d'alerte **a personnellement connaissance** des faits qu'il révèle ou signale (*il ne peut donc pas servir d'intermédiaire et doit rapporter des faits qu'il a personnellement constatés et qui lui paraissent devant être révélés ou signalés*) ;
- Le lanceur d'alerte agit **de manière désintéressée** (il ne bénéficie d'aucun avantage et ne pourra se voir attribuer une récompense financière en contrepartie de sa démarche) ;
- Le lanceur d'alerte agit **de bonne foi** (*les faits révélés ou signalés ne doivent pas chercher à nuire à autrui*).

▪ **Le lanceur d'alerte ne subit aucune conséquence liée à son signalement**

Le lanceur d'alerte agissant de bonne foi et de manière désintéressée ne pourra être licencié, sanctionné ou discriminé d'aucune manière pour avoir signalé des faits dans le respect de la présente procédure, et ce même si les faits s'avéraient par la suite inexacts ou ne donnaient lieu à aucune suite.

A l'inverse, l'utilisation abusive du dispositif d'alerte expose le lanceur d'alerte à des sanctions disciplinaires et, le cas échéant, à des poursuites judiciaires.

▪ **Le lanceur d'alerte ne verra pas son identité divulguée**

Le Groupe veille, dans le cadre du traitement de l'alerte, au respect de **la plus stricte confidentialité** concernant l'identité de l'émetteur de l'alerte. Les éléments de nature à identifier l'émetteur de l'alerte ne peuvent être divulgués, sauf à l'autorité judiciaire, qu'avec le consentement de celui-ci.

▪ **L'information du lanceur d'alerte**

Le lanceur d'alerte est informé sans délai de la bonne réception de l'alerte par un message électronique avec accusé de réception. La Cellule d'Orientation et de Traitement des Alertes (COTA) dispose alors d'un **délai de quinze jours [15 jours]** pour répondre sur la recevabilité ou pas de l'alerte.

Le Groupe dispose d'un délai légal de **trois mois [3 mois]** maximum pour se prononcer sur la recevabilité de l'alerte. A défaut d'une réponse dans ce délai, le lanceur d'alerte aura alors la faculté de s'adresser à

l'autorité judiciaire, administrative ou aux ordres professionnels. En dernier ressort, le lanceur d'alerte dispose de la faculté de rendre son alerte publique.

Le lanceur d'alerte est informé par message électronique de la clôture des opérations de vérification.

Le lanceur d'alerte est informé de la destruction ou de l'archivage des données qui s'effectuera, après anonymisation et dans un délai de **deux mois [2 mois]** à compter de la clôture des opérations de vérification.

Le Groupe met à disposition du lanceur d'alerte un espace de discussion en ligne disponible sur lequel il pourra échanger avec la Cellule d'Orientation et de Traitement des Alertes (COTA) ou lui envoyer des documents et preuves complémentaires.

Le Groupe reste très vigilant quant à la réunion des preuves ou documents collectés.

Le Compliance Officer Editis informera tout signalement au représentant du personnel désigné au sein du Comité d'Ethique Editis.

2. La personne mise en cause

▪ **L'information et la protection de la personne mise en cause**

Dès l'enregistrement des données la concernant, la personne visée par l'alerte doit être informée du traitement de ces données, afin de lui permettre notamment d'exercer ses droits d'accès, d'opposition, de rectification ou de suppression des données. Dès lors qu'il paraît nécessaire d'adopter des mesures conservatoires afin de prévenir la destruction de preuves, **l'information de la personne visée par l'alerte interviendra à postériori.**

La personne visée par l'alerte ne peut en aucun cas avoir connaissance de l'identité du lanceur d'alerte.

La personne visée par une alerte verra son identité traitée de manière **strictement confidentielle.**

Les éléments de nature à identifier la personne visée par une alerte ne peuvent pas être divulgués, sauf à l'autorité judiciaire, si après enquête il est établi le caractère fondé de l'alerte.

▪ **La protection des données à caractère personnel**

Les lanceurs d'alerte et les personnes mises en cause disposent d'un droit de rectifier, compléter, mettre à jour, verrouiller ou effacer les données à caractère personnel le concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation sont interdites.

Ils peuvent également définir des directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès.

Pour exercer ces droits, le lanceur d’alerte ou la personne mise en cause adresse sa demande comme suit :

- Par courrier recommandé, daté et signé, au siège social du Groupe Vivendi, à l’attention du Chief Data Officer, 42 avenue de Friedland 75380 Paris Cedex 08.
- Par envoi d’un e-mail à l’adresse électronique alerte@vivendi.com, en mentionnant son nom, son adresse et le numéro de téléphone auquel il peut être joint.

Il joint à sa demande une copie recto verso de sa carte d’identité ou de son passeport.

Les données faisant l’objet d’une alerte n’entrant pas dans le champ du dispositif **sont détruites sans délai, après anonymisation.**

Les données ne faisant pas l’objet d’une suite après enquête **sont détruites ou archivées, après anonymisation, dans un délai de deux mois (2 mois]** à compter de la clôture des opérations de vérification.

Le lanceur d’alerte et la personne visée par l’alerte sont informés de cette clôture.

Lorsqu’une procédure disciplinaire ou des poursuites judiciaires sont engagées à l’encontre de la personne mise en cause ou de l’émetteur d’une alerte abusive, les données relatives à l’alerte **sont conservées jusqu’au terme de la procédure, conformément aux dispositions du Règlement Général sur la Protection des Données (RGPD).**

3. La Cellule d’Orientation et de Traitement des Alertes (COTA)

- **Composition** :

- *Membres du Groupe* :

- Direction RSE & Compliance
- Direction juridique
- Direction des Ressources Humaines
- Direction Audit de Conformité
- Direction de la communication

- *Membres Editis* :

- Compliance officer
- Représentants des directions Editis

- **Mission** :

- Recueil et analyse des signalements reçus avec un accès sécurisé à la plateforme.
- Point de contact avec le lanceur d’alerte.
- Détermination des investigations à mener et conduite de l’enquête (*avec éventuel appui d’un expert*).
- Transmission du rapport d’investigation au Chief Compliance Officer.

Comment est effectué le traitement de l'alerte professionnelle ?

