

# Procédure de recueil et de traitement des alertes à destination des lanceurs d'alerte

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 » ainsi qu'aux dispositions de la loi n°2017-399 du 27 mars 2017 dite « Loi sur le devoir de vigilance », Vivendi a mis en place un dispositif d'alerte professionnelle (« le Dispositif ») qui est une plateforme commune à toutes les entités du groupe : **alerte.vivendi.com**

Il est à préciser que le Dispositif garantit par ailleurs sa conformité :

- Au règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (le « Règlement général sur la protection des données » ou « RGPD ») entré en vigueur le 25 mai 2018 ;
- Aux exigences réglementaires françaises et plus particulièrement à la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, ainsi qu'aux recommandations de la Commission Nationale de l'Informatique et des Libertés (CNIL).
- Aux recommandations de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) en matière de sécurité des systèmes d'information
- Aux recommandations de l'AFA (Agence Française Anticorruption)

Les dispositions de la présente procédure concernant le Dispositif et notamment les conditions liées au statut protecteur du lanceur d'alerte feront l'objet de mises à jour en fonction des évolutions réglementaires susceptibles d'intervenir ultérieurement à la mise à jour du Dispositif.

## 1. Le champ d'application du dispositif d'alerte professionnel

---

Le Dispositif mis en place au sein du Groupe Vivendi couvre les alertes relatives aux manquements et atteintes suivants :

- **Manquements relatifs à la violation du Code Anticorruption (article 17 de la loi dite « Loi Sapin II »)**
  - L'existence de conduites ou de situations contraires au Code de conduite anticorruption du Groupe, dans la mesure où celles-ci sont susceptibles de caractériser des faits de corruption ou de trafic d'influence.
- **Autres manquements (article 6 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.



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 »).

- **Atteintes graves liées aux activités du groupe ou de celles de ses sous-traitants et fournisseurs** envers les droits humains et les libertés fondamentales (dont discrimination, harcèlement moral et sexuel), la santé et la sécurité des personnes ainsi que l'environnement (article 1 de la loi sur le devoir de vigilance du 27 mars 2017)
- **Autres manquements** : pratiques anticoncurrentielles, violation de sanctions internationales

## 2. Les modalités du dispositif d'alerte

---

### 2.1 - Le lanceur d'alerte

Sont visés au titre de lanceur d'alerte :

- Les membres du personnel de Vivendi et de ses filiales ainsi que leurs collaborateurs extérieurs et occasionnels afin de signaler toutes conduites ou situations contraires au Code anticorruption du groupe, en application 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 (dite « loi Sapin 2 ») ;
- Les membres du personnel de Vivendi et de ses filiales ainsi que leurs collaborateurs extérieurs et occasionnels afin de signaler un crime ou un délit, une violation grave et manifeste 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, de la loi ou du règlement, ou une menace ou un préjudice grave pour l'intérêt général, en application de 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 (dite « loi Sapin 2 ») ;
- Les membres du personnel de Vivendi et de ses filiales ainsi que leurs collaborateurs extérieurs et occasionnels afin de signaler l'existence de pratiques anticoncurrentielles ou de violation de sanctions économiques internationales dans le cadre des activités du groupe.
- Toute personne, afin de signaler une atteinte grave aux droits humains et libertés fondamentales (dont discrimination, harcèlement moral et sexuel), à la santé et la sécurité des personnes ainsi qu'à l'environnement qui résulterait des activités de Vivendi ou de ses filiales, ainsi que des activités de leurs sous-traitants ou fournisseurs avec lesquels elles entretiennent une relation commerciale établie, en application de la loi n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre (dite « loi sur le devoir de vigilance »).

#### ➤ **Les conditions applicables au lanceur d'alerte pour bénéficiaire du statut de protecteur dans le cadre du dépôt d'une alerte**

Dans le cadre des alertes émises au titre d'un manquement prévu par la loi Sapin 2, le lanceur d'alerte bénéficie d'un statut protecteur subordonné aux quatre conditions cumulatives :

- 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*).

### ➤ **La protection du lanceur d'alerte**

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

Le lanceur d'alerte, personne physique, 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 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 dispositif garantit une stricte confidentialité de l'identité du lanceur d'alerte, des personnes visées par l'alerte et de toutes les informations et documents recueillis via le dispositif. Sauf, en cas de communication à l'autorité judiciaire :

- Les éléments de nature à identifier le lanceur d'alerte ne peuvent être divulgués qu'avec son consentement.
- Les éléments de nature à identifier la(les) personne(s) mise(s) en cause ne peuvent être divulgués qu'une fois que le caractère fondé de l'alerte aura été établi.

### ➤ **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.

Le Référent Principal de l'Alerte (RPA) dispose alors :

- D'un délai raisonnable pour se prononcer sur la recevabilité de l'alerte ; et
- D'un délai de trois mois [3 mois] maximum pour se prononcer sur le traitement de l'alerte et informer le lanceur d'alerte par message électronique de la mesure envisagée ou prise à titre de suivi de l'alerte. Ce délai ne constituant pas une limite pour assurer un traitement exhaustif de l'alerte.

En cas de signalement jugé irrecevable ou de classement sans suite, le lanceur d'alerte, ainsi que la personne mise en cause si elle a été informée d'un signalement la concernant, sont informés de la clôture des opérations de recevabilité et/ou de vérification des faits signalés, ainsi que de l'anonymisation de tout élément permettant leur identification, qui doit intervenir dans un délai maximum de deux mois [2 mois] à compter de la clôture des opérations de recevabilité ou vérification.

### ➤ **Les modalités d'échange avec le lanceur d'alerte**

Le Groupe met à disposition du lanceur d'alerte un espace de discussion en ligne disponible sur lequel il pourra échanger avec un référent en charge de son alerte et envoyer des documents et preuves complémentaires. Le Groupe reste très vigilant quant à la réunion des preuves ou documents collectés qui doivent obligatoirement être déposés sur la plateforme d'alerte afin de permettre de garantir les conditions de confidentialité et de sécurité de ces documents.

## **2.2 - La personne mise en cause**

### ➤ **Information et 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 a posteriori.

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.

## 2.3 - La protection des données à caractère personnel

### ➤ Les droits d'accès, de rectification et de suppression du lanceur d'alerte et de la personne mise en cause (cf. Annexe 1)

Dans le cadre de l'utilisation du dispositif d'alerte, toute personne physique dispose du droit de demander l'accès à ses données personnelles, la rectification et, si les conditions sont remplies, l'effacement de celles-ci, une limitation de leur traitement, le droit de s'opposer audit traitement et le droit à la portabilité de ses données. Toute personne concernée peut exercer ses droits en écrivant à l'adresse électronique [privacy@vivendi.com](mailto:privacy@vivendi.com), en indiquant sa demande précisément et en y joignant un justificatif d'identité. En tout état de cause, toute personne concernée peut, à tout moment, saisir l'autorité compétente (la CNIL) pour toute réclamation ou plainte quant au traitement de ses données personnelles ».

### ➤ L'anonymisation et la conservation des données à caractère personnel

Trois cas sont à distinguer :

- Lorsque le signalement est jugé irrecevable, les Données à caractère personnel y afférentes sont anonymisées dans un délai de deux (2) mois maximum suivant la clôture des opérations de recevabilité portant sur ledit signalement.
- Lorsque le signalement est jugé recevable, mais qu'aucune suite n'y est donnée, les Données à caractère personnel y afférentes sont anonymisées dans un délai de deux (2) mois suivant la clôture des opérations de vérification portant sur ledit signalement.
- Lorsque le signalement est jugé recevable et qu'une suite y est donnée, notamment qu'une procédure disciplinaire ou contentieuse est engagée à l'encontre de la personne mise en cause et/ou de l'auteur du signalement, les Données à caractère personnel y afférentes sont conservées jusqu'au terme de ladite procédure. A l'issue de cette procédure, les Données à caractère personnel sont archivées pendant la durée de prescription légale applicable compte tenu des faits signalés ou toute autre durée de conservation obligatoire découlant d'un texte législatif ou réglementaire. A l'issue de cette période d'archivage, les Données à caractère personnel sont ensuite anonymisées.

Il est rappelé que l'archivage des données s'effectue sous forme d'archive intermédiaire et que les données ainsi archivées ne pourront être consultées que de manière ponctuelle et motivée par des personnels de Vivendi et /ou de la filiale concernée spécifiquement habilités pour ce faire. Les durées d'archivage sont déterminées au regard de la catégorie des faits signalés (cf. Annexe 2).

## 3. Le lancement de l'alerte

---

### 3.1 le dépôt de l'alerte

Le dispositif d'alerte mise à disposition par le Groupe Vivendi permet d'adresser des signalements selon les catégories de faits définies sur la plateforme d'alerte.

#### ➤ 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

Lorsque l'auteur du signalement a renseigné son adresse e-mail :

- Une fenêtre pop-up apparaît au moment de l'enregistrement de son signalement précisant le numéro de dossier attribué et l'identifiant ainsi que le lien permettant à l'auteur du signalement de créer son mot de passe lui permettant d'accéder à son espace personnel via le Dispositif ; et

- Un message de confirmation automatique lui est adressé dès l'enregistrement de son signalement, qui comporte le numéro de dossier attribué et l'identifiant ainsi que le même lien permettant à l'auteur du signalement de créer son mot de passe lui permettant d'accéder à son espace personnel via le Dispositif. Ce message intègre également le récépissé confirmant la réception du signalement

Le lanceur d'alerte peut rester anonyme sous deux conditions :

- La gravité des faits mentionnés est établie  
*ET*
- Les éléments factuels sont suffisamment détaillés

Lorsque l'auteur du signalement a souhaité conserver l'anonymat, une fenêtre pop-up apparaît au moment de l'enregistrement de son signalement précisant le numéro de dossier attribué et l'identifiant ainsi que le lien permettant à l'auteur du signalement de créer son mot de passe lui permettant d'accéder à son espace personnel via le Dispositif. Cette fenêtre pop-up intègre également un lien permettant de télécharger le récépissé confirmant la réception du signalement.

### ➤ Une fois l'alerte enregistrée dans la plateforme

Le lanceur d'alerte peut se connecter à son dossier pour suivre le traitement de son alerte, par un changement de statut :

Statut	Définition
En attente	L'alerte a bien été enregistrée sur la plateforme et doit être examinée pour déterminer sa recevabilité
En cours	L'alerte a été qualifiée de recevable par le référent est en cours de traitement par la Cellule d'Enquête.
Clôturé - Archivé	Le dossier relatif à l'alerte a été clôturé et a été archivé
Clôturé - Anonymisé	Le dossier relatif à l'alerte a été clôturé et toutes les données à caractère personnel ont été anonymisées

## 3.2 - L'irresponsabilité du lanceur d'alerte

La divulgation d'un secret entraîne l'irresponsabilité pénale du lanceur d'alerte lorsque celle-ci est nécessaire et proportionnée à la sauvegarde des intérêts en cause (i) ; respecte la procédure de l'alerte (ii) ; est faite par une personne répondant aux critères du lanceur d'alerte (iii).

L'irresponsabilité pénale reste exclue pour la divulgation d'un secret de la défense nationale, d'un secret médical et d'un secret issu des relations entre un avocat et son client.

## 3.3 - La réception et l'examen de l'alerte par le Référent Principal de l'Alerte (RPA)

Par le biais de la plateforme mise à la disposition des collaborateurs (alerte.vivendi.com), le Référent Principal de l'Alerte prend connaissance de l'alerte et en informe la Direction Compliance de Vivendi qui notifie au Compliance Officer local la réception d'un signalement concernant sa filiale. Ce dernier appuie le RPA dans l'étude de la recevabilité du signalement.

### ➤ Le lanceur d'alerte reçoit un accusé réception après avoir enregistré son alerte.

Le RPA procède à l'examen de la recevabilité de l'alerte à compter de la date de réception sur la plateforme.

L'émetteur de l'alerte peut suivre le cheminement de son alerte sur la plateforme via les mentions :

- *En attente*
- *En cours*
- *Clôturé – Archivé*
- *Clôturé - Anonymisé*

### ➤ **La demande de pièces complémentaires via la plateforme**

Dans le cas où l'alerte émise par le lanceur sur la plateforme ne suffit pas à juger de sa recevabilité, le RPA peut être amené à demander des pièces justificatives ou complémentaires au lanceur d'alerte (par le biais d'un espace de discussion).

Dans le cas d'un classement de l'alerte, les éléments de l'investigation sont anonymisés dans un délai de 2 mois. Dans le cas d'une poursuite de l'enquête, ces informations sont transmises à la Cellule d'Enquête.

## **3.4 – La conduite de l'enquête interne**

### ➤ **L'information et la décision de conduite d'une enquête par la Cellule d'Enquête**

Dès lors qu'une alerte est jugée recevable, il est orienté par le RPA vers la Cellule d'Enquête « Compliance » ou la Cellule d'enquête « RH ». La Cellule d'enquête concernée réunit ses membres (les référents secondaires) composés des représentants du siège et des représentants des filiales concernés .

#### **En présence de faits probants**

A partir de l'analyse des éléments réunis par les RPA, la Cellule d'Enquête peut être amenée à constater qu'il existe suffisamment d'indices ou de faits probants pour qu'une enquête soit engagée.

#### **A défaut de preuves suffisantes**

De l'analyse des éléments réunis par le RPA, la Cellule d'Enquête ne peut pas confirmer les faits que le lanceur d'alerte a signalés et décide alors de :

- Solliciter des éléments et pièces complémentaires,

Ou

- Classer l'alerte.

### ➤ **La conduite d'une enquête**

La Cellule d'Enquête, sur la base des éléments réunis, décide de l'ouverture d'une enquête en lien avec le Compliance Officer de la filiale concernée qui associe les représentants de la filiale pour l'aider dans l'enquête. Il pourra être fait appel à un expert indépendant, pour mener tout ou partie de l'enquête notamment en présence d'éléments complexes (exemples : expertises informatiques, audit comptable, etc.).

La conduite de l'enquête est réalisée dans le respect de la confidentialité de l'auteur de l'alerte, des personnes visées et des informations recueillies. Elle est réalisée dans le respect des exigences liées aux procédures d'enquête existantes par ailleurs notamment les enquêtes en matière sociale.

### ➤ **Réalisation des entretiens**

L'audition est menée par le Compliance Officer ou toute personne désignée à cet effet, qui en garantit l'absolue confidentialité, et a pour objet la vérification des faits dans lesquels la personne mise en cause serait impliquée. Toute personne susceptible d'apporter des éléments contribuant à révéler le caractère avéré ou non des faits reprochés à la personne mise en cause peut être entendue dans le cadre de l'enquête.

La personne mise en cause est en droit de se défendre afin de révéler l'exactitude des faits.

Au terme de l'audition, un compte-rendu sera rédigé par Le Compliance Officer ou toute personne désignée à cet effet, validé par la personne mise en cause et joint au rapport d'enquête. La personne mise en cause est tenue informée des suites données à l'enquête.

### ➤ Rédaction d'un rapport d'enquête et décision de la Cellule d'Enquête

Un rapport est obligatoirement rédigé à l'issue des investigations menées dans le cadre de l'alerte. Ce rapport est remis à la cellule d'enquête qui décide des suites à donner à l'enquête.

**En cas de défaut de preuves suffisantes :** La Cellule d'Enquête ne peut pas confirmer les faits signalés par le lanceur d'alerte et décide alors de classer l'alerte.

**En présence de faits probants :** La Cellule d'Enquête peut être amenée à constater qu'il existe suffisamment de preuves pour confirmer les faits que le lanceur d'alerte a signalés. Elle émet un avis sur les suites à donner qui est transmis au Chief Compliance Officer.

## 3.5 – Suites de l'enquête

L'ensemble des éléments relatifs au traitement de l'alerte (rapport d'enquête, avis de la Cellule d'Enquête, suggestions des suites à donner) sont transmis au Chief Compliance Officer du groupe qui valide la décision d'application d'une mesure disciplinaire ou d'un dépôt de plainte.

Le Chief Compliance Officer informe le Président du Directoire de Vivendi des suites qui auront été données à l'alerte.

*Deux adresse de courriers électroniques sont associées à la plateforme du dispositif d'alerte :*

*L'adresse [compliance@vivendi.com](mailto:compliance@vivendi.com) qui 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)*

*L'adresse [privacy@vivendi.com](mailto:privacy@vivendi.com) qui a pour but de demander l'accès, la rectification ou la suppression des données concernant le lanceur d'alerte*

*Les destinataires de ces adresses électroniques ont pour rôle l'administration du site (webmaster), et n'auront pas accès aux alertes enregistrées ni aux informations relatives au traitement de ces derniers.*



## **Annexe 1 – Informations données à caractère personnel**

### **Dispositif d’alerte professionnelle**

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 (« loi Sapin 2 ») et de la loi n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre (« loi Vigilance »), le groupe Vivendi (le « Groupe ») un dispositif d’alerte professionnelle.

Conformément au Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données (« RGPD ») et à la loi n° 78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés modifiée (« loi Informatique et libertés »), est ci-après détaillé l’ensemble des informations concernant tout traitement mis en œuvre dans le cadre de ce dispositif.

Les termes employés ci-après, au singulier comme au pluriel, commençant par une majuscule ont, sauf définition expresse contraire stipulée dans la présente note d’information, le sens qui leur est donné par l’article 4 du RGPD.

#### **I. Identité du Responsable du traitement**

Lorsque le signalement est émis par un membre du personnel ou collaborateur extérieur de Vivendi SE et/ou vise des faits concernant uniquement des membres de son personnel ou collaborateurs, Vivendi SE (42, Avenue de Friedland – 75380 Paris Cedex 08 – Tel : 01 71 71 10 00) agit en qualité de Responsable du traitement.

Lorsque le signalement est émis par un membre du personnel ou collaborateur extérieur de l’une quelconque des filiales de Vivendi SE et/ou vise des faits concernant des membres de son personnel ou collaborateurs, Vivendi SE et la filiale concernée agissent en qualité de Responsables du traitement conjoints. Pour toute information de contact concernant ladite filiale, veuillez vous référer au site institutionnel de celle-ci.

#### **II. Finalités et bases juridiques du Traitement**

Le dispositif d’alerte professionnelle est destiné à permettre le recueil de signalements relatifs à l’existence de conduites ou de situations contraires à la législation et réglementation applicables en matière notamment de corruption ou trafic d’influence, pratiques anticoncurrentielles, violation de sanctions économiques, atteinte aux droits humains et libertés fondamentales, mise en danger de la santé ou à la sécurité d’autrui, atteinte à l’environnement, discrimination ou encore harcèlement moral ou sexuel, ainsi qu’à traiter ces signalements de manière appropriée.

Ce dispositif est mis en place par le Groupe aux fins de se conformer aux dispositions de la loi Sapin 2 et de la loi Vigilance, ainsi que, le cas échéant, aux fins légitimes de permettre à Vivendi SE et/ou l’une quelconque de ses filiales d’être informée(s) et en mesure d’agir promptement et de manière appropriée en cas de violation de toute législation et réglementation applicable.

#### **III. Destinataires**

Les Données à caractère personnel collectées et traitées dans le cadre du dispositif d’alerte professionnelle sont d’abord adressées au Référent principal chargé de l’étude de recevabilité du signalement, ainsi qu’à son suppléant le cas échéant.

Dans le cas où l’alerte est jugée recevable, les Données à caractère personnel sont ensuite communiquées aux Référents secondaires, spécialement désignés et habilités pour traiter et gérer le signalement en fonction de la nature et de la qualification

des faits qu'il révèle, ainsi qu'à un nombre limité de membres du personnel de Vivendi SE, et le cas échéant de la filiale concernée, spécifiquement identifiés et désignés aux fins de la gestion et du traitement dudit signalement.

En tous les cas, les Données à caractère personnel collectées et traitées dans le cadre du dispositif d'alerte professionnelle peuvent, le cas échéant, être consultées par un nombre limité de personnes habilitées au sein de la Direction des Services de l'Information de Vivendi SE, de la Direction Juridique, RSE et Compliance ainsi que de la Direction Générale de Vivendi SE et/ou l'une quelconque des filiales concernées par le signalement.

Enfin, il est possible que pour les besoins des opérations de vérification des faits signalés, des prestataires externes accèdent ponctuellement aux Données à caractère personnel, lesquels sont soumis à un engagement contractuel de confidentialité.

#### **IV. Durée de conservation des Données à caractère personnel**

Les Données à caractère personnel collectées et traitées dans le cadre du dispositif d'alerte professionnelle sont conservées uniquement pendant le temps strictement nécessaire aux finalités poursuivies.

- Lorsque le signalement est jugé irrecevable, les Données à caractère personnel y afférentes sont anonymisées dans un délai de deux (2) mois maximum suivant la clôture des opérations de recevabilité portant sur ledit signalement.
- Lorsque le signalement est jugé recevable, mais qu'aucune suite n'y est donnée, les Données à caractère personnel y afférentes sont anonymisées dans un délai de deux (2) mois suivant la clôture des opérations de vérification portant sur ledit signalement.
- Lorsque le signalement est jugé recevable et qu'une suite y est donnée, notamment qu'une procédure disciplinaire ou contentieuse est engagée à l'encontre de la personne mise en cause et/ou de l'auteur du signalement, les Données à caractère personnel y afférentes sont conservées jusqu'au terme de ladite procédure. A l'issue de cette procédure, les Données à caractère personnel sont archivées pendant la durée de prescription légale applicable compte tenu des faits signalés ou toute autre durée de conservation obligatoire découlant d'un texte législatif ou réglementaire. A l'issue de cette période d'archivage, les Données à caractère personnel sont ensuite anonymisées.

Pour plus de détails sur les délais d'archivage applicables, veuillez consulter l'annexe 2.

#### **V. Les droits des Personnes concernées**

En application des articles 15 et suivants du RGPD, toute Personne concernée dont les Données à caractère personnel sont collectées et traitées via le dispositif d'alerte professionnelle dispose du droit de demander à Vivendi SE ou l'une quelconque de ses filiales lorsque le signalement est émis par l'un des membres de son personnel ou l'un de ses collaborateurs extérieurs ou bien lorsque les faits signalés concerne ladite filiale, l'accès à ses Données à caractère personnel, leur rectification et, si les conditions sont remplies, l'effacement de celles-ci, une limitation de leur traitement, le droit de s'opposer audit traitement et le droit à la portabilité de ses Données à caractère personnel. Enfin, en application de la loi Informatique et libertés, toute Personne concernée dispose du droit de définir des directives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès.

Toute Personne concernée peut exercer ses droits en écrivant à l'adresse électronique suivante : [privacy@vivendi.com](mailto:privacy@vivendi.com), en indiquant sa demande précisément et en y joignant un justificatif d'identité.

En tout état de cause, toute Personne concernée peut saisir la CNIL pour toute réclamation ou plainte concernant le Traitement de ses Données à caractère personnel.

## Annexe 2 – Délais d’archivage

Catégories des faits signalés	Durée d’archivage
Corruption	6 ans
Trafic d’influence	6 ans
Crime	30 ans
Délit	6 ans (10 ans en cas de dommage corporel)
Violation grave et manifeste 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, de la loi ou du règlement	A déterminer cas selon la durée de prescription légale applicable en fonction de la violation commise
Menace ou préjudice grave pour l’intérêt général	A déterminer selon la durée de prescription légale applicable en fonction de la menace ou le préjudice concerné
Pratiques anticoncurrentielles	5 ans
Violation de sanctions économiques	A déterminer selon la durée de prescription légale applicable en fonction de la violation commise
Atteinte aux droits humains et libertés fondamentales	6 ans (10 ans en cas de dommage corporel)
Mise en danger de la santé ou à la sécurité d’autrui	6 ans (10 ans en cas de dommage corporel)
Atteinte à l’environnement	10 ans
Discrimination, harcèlement moral ou sexuel	6 ans (10 ans en cas de dommage corporel)
Violation du Code Anticorruption du Groupe	A déterminer selon la durée de prescription légale applicable en fonction de la violation commise