

HAVIAS

GUIDE DU LANCEUR
D'ALERTE

Sommaire

1. LE CHAMP D'APPLICATION DU DISPOSITIF D'ALERTE	5
2. LES MODALITÉS DU DISPOSITIF D'ALERTE	8
A. Le lanceur d'alerte	9
B. La personne visée par l'alerte	10
C. La protection des données à caractère personnel	11
3. LE LANCEMENT DE L'ALERTE VIA LE DISPOSITIF	12
A. Le dépôt de l'alerte	13
B. La réception et l'examen de l'alerte	14
C. La conduite de l'enquête interne	15
D. Les suites de l'enquête	16
4. Annexe 1 - Notice d'informations - Données à caractère personnel	17
5. Annexe 2 - Délais d'archivage	21

Introduction

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 », Havas a mis en place un dispositif d'alerte professionnelle (« le Dispositif ») qui est une plateforme commune à toutes les entités du groupe disponible sur le site intranet via l'adresse suivante : havas.integrityline.com

Tout Collaborateur peut également adresser son signalement directement à la Direction Compliance via l'adresse suivante : compliance@havas.com

Il est précisé 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 en matière de protection des données et plus particulièrement à la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée, ainsi qu'aux référentiels en matière de dispositif d'alerte professionnelle et aux recommandations de la Commission Nationale de l'Informatique et des Libertés (CNIL) ; et
- Aux recommandations de l'AFA (Agence Française Anticorruption).

Les dispositions de la présente procédure concernant le Dispositif feront l'objet de mises à jour en fonction des évolutions réglementaires susceptibles d'intervenir ultérieurement à la mise à jour du Dispositif.

1

1. LE CHAMP D'APPLICATION
DU DISPOSITIF D'ALERTE

1. LE CHAMP D'APPLICATION DU DISPOSITIF D'ALERTE

Le Dispositif est disponible en français, en anglais et en espagnol. Il est accessible pour les lanceurs d'alerte situés en France et à l'étranger.

Ce Dispositif n'a pas vocation à se substituer aux autres canaux d'alerte existants en interne (hiérarchie, instances représentatives du personnel, référents dédiés, le département des ressources humaines, le Chief Compliance Officer) ou en externe (ex : Défenseur des droits). Son utilisation est une alternative aux autres canaux d'alerte mais ce dernier est fortement recommandé compte tenu du fait que le Dispositif garantit la sécurité et la confidentialité du traitement de l'alerte.

Le Dispositif est accessible aux lanceurs d'alerte qui souhaitent signaler les informations, les manquements ou atteintes ci-dessous :

TYPE DE SIGNALEMENT	INFORMATIONS, MANQUEMENTS OU ATTEINTES	CATÉGORIES DE LANCEURS D'ALERTE
SIGNALEMENT RÉALISÉ DANS LE CADRE DE LA LOI DU 9 DÉCEMBRE 2016 DITE « LOI SAPIN II »	<ul style="list-style-type: none">• Conduite ou situation contraire au Code anti-corruption de Havas• Information portant sur un crime ou un délit (y compris des faits de corruption)• Information sur une menace ou un préjudice pour l'intérêt général• Information sur une violation ou une tentative de dissimulation d'une violation d'un engagement international régulièrement ratifié ou approuvé par la France mais également d'un acte unilatéral d'une organisation internationale pris sur le fondement de cet engagement• Information sur une violation ou une tentative de dissimulation d'une violation du droit de l'Union européenne, de la loi ou du règlement (y compris violation des sanctions internationales ou des règles de concurrence)	<ul style="list-style-type: none">• Membres du personnel de Havas et de ses filiales ainsi que les collaborateurs extérieurs et occasionnels• Personnes dont la relation de travail s'est terminée (dès lors que les informations ont été obtenues dans le cadre de cette relation)• Personnes candidates à un emploi au sein de l'entité concernée (dès lors que les informations ont été obtenues dans le cadre de cette candidature)• Actionnaires, associés et titulaires de droits de vote au sein de l'assemblée générale de l'entité• Membres de l'organe d'administration, de direction ou de surveillance• Co-contractants de l'entité concernée, 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 co-contractants et sous-traitants ainsi que les membres de leur personnel

TYPE DE SIGNALEMENT	INFORMATIONS, MANQUEMENTS OU ATTEINTES	CATÉGORIES DE LANCEURS D'ALERTE
<p>SIGNALEMENT RÉALISÉ DANS LE CADRE DE LA LOI DU 27 MARS 2017 DITE « LOI SUR LE DEVOIR DE VIGILANCE »</p>	<p>Sont concernées les atteintes suivantes en lien avec les activités de Havas ou de ses filiales, des sous-traitants ou fournisseurs du groupe :</p> <ul style="list-style-type: none"> • Atteinte grave aux droits humains et libertés fondamentales (y compris discrimination, harcèlement moral et sexuel) • Atteinte grave à la santé et la sécurité des personnes • Atteinte grave à l'environnement 	<ul style="list-style-type: none"> • Toute personne physique ou morale

Sont exclues du champ d'application les alertes portant sur des faits couverts par le secret de la défense nationale, le secret médical, le secret de l'enquête ou de l'instruction judiciaires et le secret professionnel de l'avocat (Article 6-2 de la loi Sapin II).

2

2. LES MODALITÉS DU DISPOSITIF D'ALERTE

2. LES MODALITÉS DU DISPOSITIF D'ALERTE

A. Le lanceur d'alerte

L'auteur d'un signalement bénéficie du statut protecteur de lanceur d'alerte sous réserve de répondre aux conditions suivantes :

- **Être une personne physique ;**
- **Agir de bonne foi :** Le lanceur d'alerte ne doit pas être animé d'une intention de nuire à autrui ;
- **Agir sans contrepartie financière :** Le lanceur d'alerte ne peut pas prétendre à être rémunéré pour son signalement ;
- **Avoir connaissance des faits :** Dans le contexte professionnel, le lanceur d'alerte peut signaler des faits dont il a eu personnellement connaissance ou qui lui ont été rapportés. Hors du contexte professionnel, le lanceur d'alerte doit avoir eu personnellement connaissance des faits qu'il signale ;
- **Être identifiable :** L'utilisation du Dispositif est soumise à l'identification du lanceur d'alerte. Par exception, l'anonymat est admis si la gravité des faits signalés est établie et si les faits sont suffisamment détaillés. Le lanceur d'alerte ne pourra bénéficier des mesures de protection (voir ci-après) qu'une fois l'anonymat levé.

LA PROTECTION DU LANCEUR D'ALERTE

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

- Sous réserve d'émettre une alerte dans le respect des dispositions prévues dans le présent guide, le lanceur d'alerte ne peut pas faire l'objet de mesures de représailles, ni de menaces ou de tentatives de recourir à ces mesures, notamment sous les formes suivantes (Article 10-1 de la loi Sapin II) :
 - Suspension, mise à pied, licenciement ou mesures équivalentes ;
 - Rétrogradation ou refus de promotion ;
 - Transfert de fonctions, changement de lieu de travail, réduction de salaire, modification des horaires de travail ;
 - Suspension de la formation ;
 - Evaluation de performance ou attestation de travail négative ;
 - Mesures disciplinaires imposées ou administrées, réprimande ou autre sanction, y compris une sanction financière ;
 - Coercition, intimidation, harcèlement ou ostracisme ;
 - Discrimination, traitement désavantageux ou injuste ;
 - Non-conversion d'un contrat de travail à durée déterminée ou d'un contrat temporaire en un contrat permanent, lorsque le travailleur pouvait légitimement espérer se voir offrir un emploi permanent ;
 - Non-renouvellement ou résiliation anticipée d'un contrat de travail à durée déterminée ou d'un contrat temporaire ;
 - Préjudice, y compris les atteintes à la réputation de la personne, en particulier sur un service de communication au public en ligne, ou pertes financières, y compris la perte d'activité et la perte de revenu ;
 - Mise sur liste noire sur la base d'un accord formel ou informel à l'échelle sectorielle ou de la branche d'activité, pouvant impliquer que la personne ne trouvera pas d'emploi à l'avenir dans le secteur ou la branche d'activité ;
 - Résiliation anticipée ou annulation d'un contrat pour des biens ou des services ;
 - Annulation d'une licence ou d'un permis ;
 - Orientation abusive vers un traitement psychiatrique ou médical.

- Le lanceur d’alerte bénéficie de l’irresponsabilité civile et pénale
 - Le lanceur d’alerte n’est pas responsable au civil et ne pourra pas être condamné à verser des dommages et intérêts pour les dommages causés du fait de son signalement ou de sa divulgation publique dès lors qu’il avait des motifs raisonnables de croire que le signalement ou la divulgation publique des informations était nécessaire à la sauvegarde des intérêts en cause.
 - Le lanceur d’alerte n’est pas responsable pénalement s’il 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 procédures de signalement définies par la loi et que la personne répond aux critères de définition du lanceur d’alerte prévus par la loi.
- Ce statut protecteur bénéficie également aux personnes physiques ou morales qui sont en lien avec le lanceur d’alerte :
 - Facilitateurs : personne physique ou morale de droit privé à but non lucratif qui aide à effectuer le signalement ou la divulgation (ex : représentants syndicaux, représentants du personnel) ;
 - Personne physique en lien avec le lanceur d’alerte (ex : collègues, proches) ;
 - Entités juridiques contrôlées par le lanceur d’alerte pour laquelle il travaille ou est en lien dans un contexte professionnel.
- 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.

B. La personne visée par l’alerte

INFORMATION ET PROTECTION DE LA PERSONNE VISÉE PAR L’ALERTE

Dès l’enregistrement des données la concernant, la personne visée par l’alerte doit être informée du traitement de ses données, afin de lui permettre notamment d’exercer ses droits d’accès, de rectification et, si les conditions sont remplies, d’opposition, de suppression des données, de limitation du traitement et de portabilité. 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 à ce stade.

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 le caractère fondé de l’alerte est établi.

C. La protection des données à caractère personnel

LES DROITS D'ACCÈS, DE RECTIFICATION ET DE SUPPRESSION (CF. ANNEXE 1)

Dans le cadre de l'utilisation du Dispositif, toute personne physique dispose du droit de demander l'accès à ses données à caractère personnel, 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 dpo@havas.com, en indiquant sa demande précisément et en justifiant de son identité par tout moyen. En tout état de cause, toute personne concernée peut, à tout moment, saisir l'autorité compétente en matière de protection des données à caractère personnel (En France, la CNIL) pour toute réclamation ou plainte quant au traitement de ses données à caractère personnel.

Pour en savoir plus sur les droits des personnes, il est renvoyé à l'Annexe 1 du présent document : Notice d'informations – Données à caractère personnel.

LA CONSERVATION ET L'ANONYMISATION DES DONNÉES À CARACTÈRE PERSONNEL

Trois cas sont à distinguer :

- Lorsque le signalement est jugé irrecevable, les données à caractère personnel 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 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 visée par l'alerte et/ou de l'auteur du signalement, les données à caractère personnel 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. À l'issue de cette période d'archivage, les données à caractère personnel sont ensuite anonymisées.

Il est rappelé que les données archivées ne pourront être consultées que de manière ponctuelle et motivée par des personnels de Havas 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

**3. LE LANCEMENT DE L'ALERTE
VIA LE DISPOSITIF**

3. LE LANCEMENT DE L'ALERTE VIA LE DISPOSITIF

A. Le dépôt de l'alerte

Le Dispositif mis à disposition par le Groupe Havas permet d'adresser des signalements selon les catégories de faits définies sur la plateforme d'alerte. En déposant une alerte sur la plateforme, il est possible de sélectionner plusieurs catégories si la nature des faits reportés le nécessite.

L'utilisation abusive (ex : porter de fausses accusations) ou de mauvaise foi du Dispositif peut exposer son auteur à des sanctions disciplinaires ainsi qu'à des poursuites judiciaires.

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 (les formats autorisés sont : PDF, Word, Excel, Power Point, GIF, JPEG) ;
- Communiquer toutes les données nécessaires et complémentaires demandées ;
- Renseigner son adresse e-mail pour valider l'enregistrement et créer son mot de passe personnel. Une référence unique de dossier lui sera attribuée à la fin de l'enregistrement. Veuillez à bien conserver vos identifiants et la référence du dossier afin d'avoir accès à la boîte de dialogue sécurisée. En cas de perte de la référence du dossier, il vous sera impossible de réinitialiser vos identifiants. Vous devrez alors soumettre une nouvelle alerte

Le lanceur d'alerte peut rester anonyme à condition que :

- La gravité des faits mentionnés soit établie

ET

- Les éléments factuels soient suffisamment détaillés

Lorsque l'auteur du signalement a souhaité conserver l'anonymat, il lui faudra tout de même créer un mot de passe personnel et veiller à bien conserver la référence unique de dossier qui lui sera attribuée à la fin de l'enregistrement de son alerte afin d'avoir accès à la boîte de dialogue sécurisée.

L'INFORMATION DU LANCEUR D'ALERTE

À compter du dépôt du signalement sur la plateforme d'alerte :

- Le lanceur d'alerte reçoit, dans un délai maximum de sept (7) jours, un accusé de réception dans la boîte de dialogue sécurisée qui lui notifie l'enregistrement de son signalement.
- Le lanceur d'alerte est informé dans un délai maximum de trois (3) mois à compter de l'accusé de réception sur les mesures envisagées ou prises pour évaluer l'exactitude des allégations et, le cas échéant, remédier à l'objet du signalement. Le lanceur d'alerte peut suivre à tout moment, à partir de son espace personnel, l'état d'avancement du traitement de l'alerte :
 - Si l'alerte est irrecevable → Le dossier est clôturé pour irrecevabilité.
 - Si l'alerte est recevable → La Direction Compliance Groupe, au regard de la nature des faits signalés et conformément aux procédures locales, procède à la mise en état du dossier pour identifier et mener les investigations nécessaires et, le cas échéant, les mesures à mettre en œuvre.

- Le délai de traitement est porté à six (6) mois si les circonstances particulières du signalement, liées notamment à sa nature ou à sa complexité, nécessitent des investigations complémentaires. Le lanceur d’alerte en est informé avant l’expiration du délai de trois (3) mois initial.

LES MODALITÉS D’ÉCHANGE AVEC LE LANCEUR D’ALERTE

Le lanceur d’alerte dispose d’un espace de discussion en ligne sur lequel il pourra échanger avec un référent compliance 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.

B. La réception et l’examen de l’alerte

Une fois l’alerte enregistrée sur la plateforme d’alerte (havas.integrityline.com), la Direction Compliance Groupe en prend connaissance. Elle examine la recevabilité de l’alerte au regard des éléments suivants :

- Caractéristiques du signalement ;
- Informations fournies sur le signalement ;
- Critères applicables au lanceur d’alerte (cf.§2.A).

Les étapes du traitement de l’alerte, sont les suivantes :

STATUT	ETAT DU DOSSIER
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 et est en cours de traitement par la Direction Compliance Groupe
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

LA DEMANDE DE DOCUMENTS COMPLÉMENTAIRES VIA LA PLATEFORME

Dans le cas où l’alerte émise par le lanceur d’alerte sur la plateforme ne suffit pas à juger de sa recevabilité, le référent compliance peut être amené à demander des pièces justificatives ou complémentaires au lanceur d’alerte (par le biais d’un espace de discussion). Ainsi, il pourra lui demander de fournir un document justifiant de son profil en tant que lanceur d’alerte (salarié, actionnaire, etc.) et tout autre élément permettant d’apprécier l’exactitude des allégations.

C. La conduite de l'enquête interne

L'INFORMATION ET LA DÉCISION DE CONDUITE D'UNE ENQUÊTE PAR LA DIRECTION COMPLIANCE

Dès lors qu'une alerte est jugée recevable, la Direction Compliance Groupe met en état le dossier. Deux cas de figure se présentent :

En présence de faits probants

À partir de l'analyse des éléments transmis, la Direction Compliance Groupe peut être amenée à constater qu'il existe suffisamment d'indices ou de faits probants pour qu'une enquête soit engagée.

À défaut de preuves suffisantes

À partir de l'analyse des éléments transmis, la Direction Compliance Groupe 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 Direction Compliance Groupe, sur la base des éléments réunis, décide de l'ouverture d'une enquête qui est confiée à une cellule d'enquête, spécialement composée, selon la nature des faits reportés. La Direction Compliance Groupe pour mener l'enquête peut faire appel aux Directions suivantes selon les expertises requises : DRH, Direction Juridique, Direction Financière, Direction de l'Audit Interne, etc.

Il pourra être fait appel à un expert indépendant, soumis à une obligation de confidentialité, pour mener tout ou partie de l'enquête notamment en présence d'éléments complexes (exemple : 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 exemple en matière sociale.

RÉALISATION DES ENTRETIENS

Les entretiens sont menés par la cellule d'enquête ou par toute personne désignée à cet effet, garantissant leur absolue confidentialité. Ces entretiens ont pour objet la vérification des faits dans lesquels la personne visée par l'alerte serait impliquée. Toute personne susceptible d'apporter des éléments contribuant à révéler le caractère avéré ou non des faits reprochés à la personne visée par l'alerte peut être entendue dans le cadre de l'enquête.

En application du principe du contradictoire, la personne visée par l'alerte a le droit d'être entendue par la cellule d'enquête et de pouvoir répondre à l'ensemble des griefs qui la visent.

Au terme de chaque entretien, un compte-rendu sera rédigé par la cellule d'enquête ou par toute personne désignée à cet effet, validé et signé par chaque personne entendue et joint au rapport d'enquête. La personne visée par l'alerte ainsi que l'auteur du signalement sont tenus informés du déroulement de l'enquête, sur simple demande.

RÉDACTION D'UN RAPPORT D'ENQUÊTE ET SUITES A DONNER

Un rapport est obligatoirement rédigé par la cellule d'enquête à l'issue des investigations menées dans le cadre de l'alerte. Les conclusions du rapport sont notamment partagées par la cellule d'enquête avec l'auteur du signalement et la personne visée par l'alerte.

D. Les suites de l'enquête

A l'issue des investigations menés par la cellule d'enquête et de la rédaction du rapport d'enquête, trois situations peuvent se présenter :

- **Le rapport d'enquête ne permet pas de confirmer les faits signalés par le lanceur d'alerte**

Dans ce cas, la cellule d'enquête classe l'alerte. Le lanceur d'alerte est informé de son classement et des motifs qui le justifie par un message déposé sur la plateforme d'alerte.

- **Le rapport d'enquête ne permet de confirmer que partiellement les faits signalés**

La cellule d'enquête peut bénéficier d'un délai supplémentaire de trois (3) mois afin de mener des investigations complémentaires. Le lanceur d'alerte est informé par un message déposé sur la plateforme d'alerte de la poursuite des investigations à l'issue du délai de trois (3) mois initial.

- **Le rapport d'enquête démontre qu'il existe suffisamment de preuves pour confirmer les faits signalés**

Le lanceur d'alerte est alors informé, par un message déposé sur la plateforme d'alerte, des mesures envisagées ou mises en place pour évaluer l'exactitude de ses allégations et, le cas échéant, des mesures visant à remédier à l'objet du signalement ainsi que sur les motifs de ces dernières.

L'ensemble des éléments relatifs au traitement de l'alerte (rapport d'enquête, avis de la cellule d'enquête, suites données au signalement) sont conservés et archivés selon les règles internes prévues pour la protection des données à caractère personnel.

Deux adresses de courriers électroniques sont complémentaires à la plateforme du Dispositif :

L'adresse compliance@havas.com qui a uniquement pour but de permettre au lanceur d'alerte d'échanger sur le fonctionnement de la plateforme, si l'alerte a été déposée via le Dispositif.

L'adresse dpo@havas.com qui a pour but de demander l'accès, la rectification, la limitation du traitement, la portabilité ou la suppression des données concernant le lanceur d'alerte, si les conditions sont remplies.

Les demandes effectuées sur les deux adresses ci-dessus ne confèrent pas un accès au contenu de la plateforme.

Ces adresses électroniques sont un relais externe entre les demandes formulées via celles-ci et leur gestion par le Responsable du traitement de la plateforme d'alerte.

4

**4. ANNEXE 1 - NOTICE
D'INFORMATIONS - DONNÉES
À CARACTÈRE PERSONNEL**

4 - ANNEXE 1 - NOTICE D'INFORMATIONS - DONNÉES À CARACTÈRE PERSONNEL

En application notamment 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 II ») 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 sur le devoir de vigilance »), le groupe Havas (le « Groupe ») met à disposition de toute personne un dispositif d'alerte professionnelle (le « Dispositif »).

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 pour la France 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.

A. Identité du Responsable du traitement

Lorsque le signalement est émis par un lanceur d'alerte en relation avec Havas et/ou vise des faits concernant uniquement des membres de son personnel ou collaborateurs, Havas (29-30 Quai de Dion Bouton – 92800 Puteaux - France) agit en qualité de Responsable du traitement.

Lorsque le signalement est émis par un lanceur d'alerte en relation avec l'une quelconque des filiales de Havas et/ou vise des faits concernant des membres de son personnel ou collaborateurs, Havas 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.

B. Finalités et bases juridiques du traitement

Le Dispositif 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 à la législation, notamment aux dispositions applicables de la loi Sapin II et de la loi sur le devoir de vigilance, ainsi que, le cas échéant, aux fins légitimes de permettre à Havas 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.

C. Destinataires

Les données à caractère personnel collectées et traitées dans le cadre du Dispositif 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 Havas, 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 peuvent, le cas échéant, être consultées par un nombre limité de personnes habilitées au sein de la Direction des Services de l'Information de Havas, de la Direction Juridique, RSE et Compliance ainsi que de la Direction Générale de Havas 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.

D. Durée de conservation des données à caractère personnel

Les données à caractère personnel collectées et traitées dans le cadre du Dispositif sont conservées uniquement pendant le temps strictement nécessaire aux finalités poursuivies.

- Lorsque le signalement est jugé irrecevable, les données à caractère personnel 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 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 visée par l'alerte et/ou de l'auteur du signalement, les données à caractère personnel 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.

Les détails sur les délais d'archivage applicables sont présentés dans l'Annexe 2.

E. 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 dispose du droit de demander à Havas (ou l'une quelconque de ses filiales lorsque le signalement est émis par un lanceur d'alerte en relation avec cette filiale ou bien lorsque les faits signalés concernent 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 France, en application de la loi informatique et libertés modifiée, toute personne concernée dispose du droit de définir des directives générales ou particulières relatives 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 : dpo@havas.com, en indiquant sa demande précisément et en justifiant de son identité par tout moyen.

En tout état de cause, toute personne concernée peut saisir l'Autorité compétente en matière de protection des données à caractère personnel (en France, la CNIL) pour toute réclamation ou plainte concernant le traitement de ses données à caractère personnel.

5

5. ANNEXE 2 – DÉLAIS D'ARCHIVAGE

5. 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 ANTI-CORRUPTION DU GROUPE	A déterminer selon la durée de prescription légale applicable en fonction de la violation commise



HAVIAS