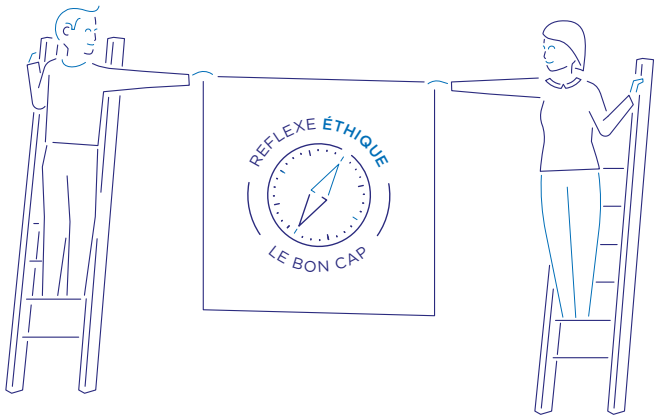
GROUPE ADP

DES HORIZONS À PARTAGER

CHARTE DE TRAITEMENT DES ALERTES

ÉTHIQUE ET COMPLIANCE

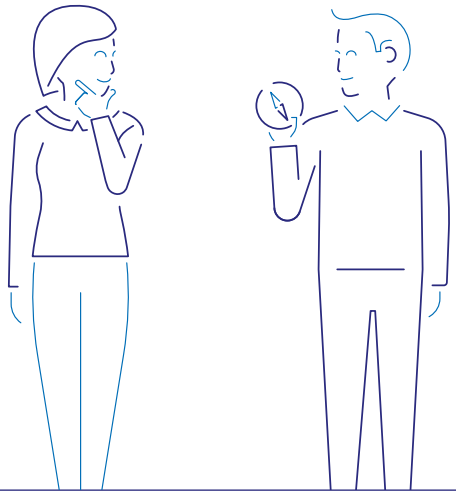


La plateforme est accessible 24h/24, 7j/7 (https://alert.groupeadp.fr) dans la langue locale des pays dans lesquels le Groupe ADP opère.

La plateforme est le moyen prioritaire pour remonter une alerte.

Les alertes peuvent être anonymes dans le respect des règles de la présente charte

SOMMAIRE



PRÉAMBULE

La présente Charte décrit le dispositif d'alerte interne déployé au sein du Groupe ADP. Elle définit le **champ d'application du dispositif, les modalités de fonctionnement** de celui-ci, **les conditions d'utilisation et de conservation des données à caractère personnel** susceptibles d'être recueillis dans le cadre du dispositif. Elle décrit également les garanties offertes pour assurer **la protection des personnes** dès la réception de l'alerte.

Au-delà de l'accessibilité, la confiance est un prérequis pour que le dispositif d'alerte soit effectif et utilisé. Le niveau de notoriété et de confiance dans le dispositif sera mesuré a minima tous les ans au travers d'un Baromètre du Climat Éthique.

Le dispositif d'alerte interne fait partie du programme Éthique et Compliance mis en place par Aéroports de Paris et déployé au sein du Groupe ADP. Il est décrit dans le Code de Conduite (annexé au Règlement Intérieur d'Aéroports de Paris qui a été soumis à consultation du CSE. Pour les filiales il est déployé suivant les moyens les plus appropriés localement). L'Éthique et la Compliance impliquent que chaque collaborateur adopte un comportement conforme aux lois, aux règlements, aux règles internes et plus généralement aux valeurs du groupe.

Ce dispositif contribue à la protection des collaborateurs et de l'entreprise contre les différents risques auxquels ils sont exposés (humains, financiers, juridiques, réputationnels, etc.) mais également dans une optique de défense commune et solidaire de l'intérêt général.

L'objectif du dispositif d'alerte interne est de recueillir les alertes internes provenant des collaborateurs du Groupe ADP et également les alertes externes issues des entités identifiées dans le présent document. Il est également possible d'effectuer un signalement « en externe », dans les conditions fixées par le décret n° 2022-1284 du 3 octobre 2022, à l'une des 45 autorités désignées par ledit décret, ou à l'autorité judiciaire ou encore directement auprès du Défenseur des droits.

Le signalement peut également être directement rendu public ou adressé à l'autorité judiciaire en cas de danger imminent ou manifeste pour l'intérêt général ou lorsque le signalement interne ou externe ne peut permettre de remédier efficacement à l'objet de la divulgation ou qu'il fait encourir à son auteur un risque de faire l'objet de mesures de représailles mentionnées à l'article 10-1 de la loi Sapin II, ou en raison des circonstances particulières de l'affaire, comme lorsque des preuves peuvent être dissimulées ou détruites ou lorsque l'auteur du signalement a des motifs sérieux de penser que l'autorité peut être en conflit d'intérêts ou en collusion avec l'auteur de la violation ou impliquée dans la violation.

La nature des alertes peut concerner des violations de la loi ou des manquements aux dispositions du code de conduite du Groupe et plus généralement, sur tout manquement en matière de libertés fondamentales et droits de l'homme, d'environnement et de santé et sécurité du travail.

Le cadre juridique du dispositif d'alerte mis en place repose sur l'ensemble des lois des pays dans lesquels le dispositif sera déployé et notamment en ce qui concerne l'Europe et la France sur :

- La Directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union qui vise à améliorer la protection des lanceurs d'alerte et à créer un cadre commun de protection au sein de l'Union Européenne transposée dans deux lois (Loi n° 2002-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alertes et Loi organique n° 2022-400 du 21 mars 2022 visant au renforcement du rôle du Défenseur des droits en matière de signalement d'alerte) qui ont amené à la modification de la loi Sapin II.
- 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 » (reconnaissant le statut du lanceur d'alerte et la nécessité de le protéger).
- Le décret d'application n° 2022-1284 du 3 octobre 2022 pour l'application de la loi Waserman relatif aux procédures de recueil et de traitement des signalements émis par les lanceurs d'alerte et fixant la liste des autorités externes instituées par la loi n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte en définissant ce qui est considéré comme représailles.
- La loi n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et entreprises donneuses d'ordre traitant de l'environnement et des droits humains.

LES 4 PILIERS DU DISPOSITIF D'ALERTE

- La **protection de la personne à l'origine de l'alerte et des facilitateurs** dès lors qu'ils agissent de bonne foi suivant l'article 6 de la loi du 9 décembre 2016.
- La **présomption d'innocence** des personnes visées par l'alerte.
- La **bonne conduite** des parties impliquées dans le recueil et le traitement de l'alerte.
- Le respect de la **confidentialité** des personnes et des faits.

Toute entrave à l'exercice du droit d'alerte est sanctionnée pénalement (jusqu'à un an d'emprisonnement et 15 000 € d'amende).

1/ Comment utiliser le dispositif d'alerte ?

1.1. Définition du dispositif d'alerte

Le dispositif d'alerte mis en place dans le cadre défini ci-dessus constitue un moyen d'expression supplémentaire quel que soit le canal d'alerte (plateforme, téléphone, etc.) choisi et indépendamment du dialogue avec les managers ou le réseau RH. Il peut être utilisé par des personnes internes ou externes au Groupe ADP autorisées à déposer un signalement de façon anonyme ou non.

Il permet de :

- Formuler une demande ou une question relative à l'Éthique ou à la Compliance ou obtenir une aide devant un questionnement ou une situation délicate. A priori, les questions, sauf si elles aboutissent sur une alerte, ne sont pas considérées comme des alertes recevables. Elles devront cependant recevoir une réponse via la plateforme (si l'alerte y est déposée) dans un délai maximum de 3 mois.
- Signaler des faits portant sur l'un des domaines entrant dans son champ d'application.

1.2. Les acteurs du dispositif d'alerte

Le dispositif est piloté par la **Direction de l'Ethique et Données Personnelles du Groupe** et en particulier par les personnes désignées en annexe de la présente Charte. Seules les personnes désignées sont habilitées à accéder à toutes les alertes de la plateforme d'alerte. Dans certains cas et à leur initiative, elles peuvent donner certains accès aux référents Ethique et Compliance pour le périmètre qui les concerne, et aux enquêteurs du Groupe ADP.

Les référents éthiques & compliance sont les personnes identifiées comme étant les interlocuteurs privilégiés dans le traitement des alertes. Afin de garantir l'impartialité et la confidentialité de toutes les personnes impliquées dans le processus de traitement, elles signent un engagement de confidentialité et appliquent les principes de la présente charte. Les référents éthiques & compliance d'Hub One, AIG, TAV Airports (cf. annexe) peuvent être récepteurs directs d'une alerte locale, dont ils doivent informer la Direction Ethique et Données personnelles du Groupe afin qu'elle soit remise sur la plateforme.

Les managers qui reçoivent des alertes doivent en informer la Direction de l'Ethique et des données personnelles dans la mesure où la loi locale et les restrictions de confidentialité le permettent. À cette fin, des conseils doivent être fournis aux managers afin qu'ils disposent d'instructions claires sur la manière de traiter ces alertes et sur le moment où ils doivent les signaler.

La Direction des Ressources Humaines informe la Direction de l'Ethique et des données personnelles des alertes reçues suivant les dispositions définies entre ces deux entités afin de garantir, dans la mesure du possible, une exhaustivité des alertes et du traitement qui en est fait.

Le Comité de traitement ad hoc est mis en place pour chaque alerte recevable. Il réunira à l'initiative de la Direction Ethique et Données personnelles, un nombre limité de personnes compétentes au regard des allégations à traiter (finance, juridique, RH, etc.) qui signent également un engagement de confidentialité.

1.3. Qui peut déposer une alerte ?

Les alertes anonymes sont possibles. Pour être jugées recevables les alertes anonymes doivent comprendre des éléments factuels suffisamment détaillés et présenter des faits d'une gravité établie. Dans ce cas, l'alerte sera traitée de manière classique.

Les personnes autorisées à effectuer un signalement (soit via la plateforme, soit via les canaux de signalement prévus dans la présente charte) sont :

- Une personne physique.
- Les membres du personnel , CDI, CDD, stagiaires, alternants, anciens salariés et candidats lorsque les informations ont été obtenues dans le cadre de l'ancienne relation de travail ou de la candidature.
- Les collaborateurs extérieurs et occasionnels (salariés mis à disposition et intérimaires, agents et mandataires, etc.).
- Les actionnaires associés et titulaires de droits de vote au sein des assemblées générales de l'entité.
- Les membres des organes d'administration, de direction ou de surveillance.
- Les cocontractants ainsi que leurs sous-traitants de l'entité (fournisseurs, clients, etc.).

1.4. Les canaux de signalement d'alerte

Différents canaux existent pour entrer en contact avec la Directrice de l'Ethique et Données personnelles, la responsable du pôle Enquêtes, ou leurs intérims : contact direct, signalement par téléphone ou tout autre système de messagerie (vocale, réseau social professionnel…), courrier, ou via la plateforme d'alerte mise en place au niveau du Groupe ADP.

La plateforme est accessible 24h/24, 7j/7 (https://alert.groupeadp.fr) dans la langue locale des pays dans lesquels le Groupe ADP opère.

Quel que soit le canal utilisé, la demande devra in fine être formalisée à travers la plateforme d'alerte dédiée. **Ce canal doit être privilégié** dans le but de protéger le lanceur d'alerte, les facilitateurs, ou toute autre personne physique partie prenante dans le traitement de l'alerte ; cela permet aussi de préserver la confidentialité des informations recueillies et des échanges et assure la garantie de traitement des alertes.

Dans le cas, où des signalements sont reçus par d'autres personnes que celles prévues dans la présente charte, ils doivent être transmis sans délai aux personnes désignées au sein de la Direction de l'Ethique et Protection des données ou des Référents Ethique et Compliance des filiales.

1.5. Champ d'application du dispositif d'alerte

Ne peuvent être révélées au titre de l'alerte, au risque d'engager la responsabilité civile et pénale, des informations, faits ou documents relevant du secret médical, du secret professionnel des avocats, du secret de la défense nationale, du secret des délibérations judiciaires, du secret d'une enquête judiciaire, du secret d'une instruction judiciaire.

Les alertes peuvent concerner tout manquement au Règlement Intérieur (RI) dans lequel est annexé le code de conduite ou l'équivalent du code dans les filiales dont les principes essentiels sans exhaustivité sont rappelés ci-dessous :

- Respect des lois et réglementations ;
- Lutte contre les atteintes à la probité ;
- Prévention de la corruption ;
- Conflits d'intérêts ;
- Prévention des pratiques collusoires et coercitives et respect des principes de libre concurrence ;
- Prévention du trafic d'influence ;
- Cadeaux, invitations et avantages ;
- Protection de l'information et des données à caractère personnel ;
- Les menaces ou préjudices graves pour l'intérêt général. Par exemple, les atteintes graves envers les droits humains et les libertés fondamentales, la santé et la sécurité des personnes et l'environnement ;
- Respect des principes de loyauté, d'équité et d'intégrité.

Les alertes peuvent aussi concerner :

- Un crime (ex. : vol aggravé, viol, attentat) ou un délit (ex : fraude fiscale, faux en écriture, corruption, abus de biens social, abus de confiance, prise illégale d'intérêt, trafic d'influence, appels téléphoniques ou envoi de messages malveillants, menaces, harcèlement sexuel ou moral, discriminations de tout ordre, extorsion, chantage, escroquerie, usage illégal de fonds publics…).
- Une violation ou une tentative de dissimulation d'une violation d'un engagement international ou du droit de l'Union Européenne.
- Une menace ou un préjudice pour l'intérêt général ou une violation d'une loi ou d'un règlement.

2/ Droits et devoirs des parties prenantes

2.1. Principes généraux

Toutes les personnes impliquées dans l'instruction de l'alerte sont tenues à une obligation renforcée de confidentialité et à coopérer lors de l'instruction de l'alerte.

Pour bénéficier de la protection inhérente au statut de lanceur d'alerte, la personne à l'origine du signalement doit :

- Être de bonne foi (avoir la croyance raisonnable que les faits signalés sont vrais au moment de l'alerte).
- Réaliser la divulgation ou le signalement sans contrepartie financière directe.
- Préserver la confidentialité de l'alerte soumise via le dispositif.

Les facilitateurs ou certaines personnes physiques (proches, collègues, etc.) de l'entourage du lanceur d'alerte qui l'aident à effectuer un signalement bénéficient également du régime de protection prévu par la loi (notamment contre les représailles ou les mesures de soutien psychologique).

Les personnes qui exercent des représailles à l'encontre d'un lanceur d'alerte ou d'un facilitateur peuvent être condamnées à une peine de 3 ans d'emprisonnement et 45 000 euros d'amende. Aucune personne ne peut, pour avoir signalé ou divulgué des informations, faire l'objet notamment des mesures ci-dessous, ni de menaces ou de tentatives de recourir à ces mesures (le juge a la possibilité d'allouer une provision pour les frais de justice au lanceur d'alerte qui conteste une mesure de représailles ou subit une procédure « bâillon ») :

- 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.
- Évaluation 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 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 temporaire.
- Préjudice, y compris les atteintes à la réputation de la personne, en particulier sur les réseaux sociaux, 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 au niveau du secteur ou de 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 vers un traitement psychiatrique ou médical.

Toute utilisation abusive du dispositif d'alerte (exemple : dénonciation calomnieuse, diffamation) expose son auteur à des poursuites et sanctions disciplinaires. Les personnes ayant des pratiques dilatoires (ayant pour effet de retarder l'alerte ou son traitement) ou abusives peuvent être condamnées à une amende civile de 60 000 euros.

2.2. L'engagement du Comité de traitement des alertes

Pour la mise en œuvre du dispositif d'alerte les membres du Comité de Traitement remplissent leurs missions dans le respect des engagements suivants :

- Agir avec efficacité dans un souci constant de neutralité et d'impartialité. Une vérification des conflits d'intérêts sera effectuée à chaque lancement de comité,
- Considérer l'ensemble des demandes ou alertes correspondant au champ d'application du dispositif avec une attention particulière,
- Être réactif dans la prise en compte de l'alerte et dans son traitement,
- Informer la personne à l'origine de l'alerte de l'évolution de son traitement, tout en veillant à respecter les règles de confidentialité,
- Protéger les parties prenantes selon les règles décrites ci-dessous et notamment garantir la confidentialité de l'identité du lanceur d'alerte ainsi que des personnes concernées et des informations.

Ils signent tous un engagement de confidentialité leur rappelant leurs obligations et les sanctions associées. Le comité de traitement n'est constitué que des personnes strictement nécessaires au traitement de l'alerte.

3/ Les garanties de protection offertes par le dispositif

3.1. Protection des personnes à l'origine d'une alerte et des facilitateurs

Toutes les précautions sont prises par les acteurs du dispositif d'alerte en vue de garantir la stricte confidentialité des éléments de nature à identifier les personnes à l'origine d'une alerte ou un facilitateur, tant pour le recueil de l'alerte que pour son traitement.

La procédure doit assurer l'intégrité et la confidentialité des informations recueillies, « notamment l'identité de l'auteur du signalement, des personnes visées par celui-ci et de tout tiers qui y est mentionné » et en même temps empêcher que des personnes qui ne sont pas autorisées à connaître des éléments du signalement puissent y accéder. Des tiers ne peuvent connaître ces informations que si cette communication est nécessaire pour traiter le signalement, dans le respect des conditions prévues à l'article 9-I de la loi Sapin II.

Les éléments de nature à identifier le lanceur d'alerte ne peuvent être divulgués qu'avec le consentement de celui-ci, sauf à l'autorité judiciaire, auquel cas il en est informé, à moins que cette information ne risque de compromettre la procédure judiciaire concernée.

Lorsque le recours à des tiers (par exemple, un cabinet forensic) est rendu nécessaire dans le cadre du traitement de l'alerte, la Direction de l'Ethique et Données personnelles s'assure qu'ils s'astreignent à une obligation de confidentialité renforcée au même titre que les acteurs du dispositif d'alerte.

Toute rupture de confidentialité (identité, information, etc.) par les acteurs du dispositif d'alerte ou toute personne accréditée pour le traitement de l'alerte peut donner lieu à des sanctions disciplinaires et pénales (Loi Sapin II) : jusqu'à 2 ans de prison et 30 000 € d'amende. Pour rappel, ces différents acteurs ont signé un acte d'engagement.

Mesures de protection

Lorsque les personnes concernées (lanceurs d'alerte & facilitateurs) exercent leur droit de l'utilisation du dispositif d'alerte, les représailles de toute nature sont interdites et sanctionnables (exemples : l'intimidation, atteinte à la réputation notamment sur les réseaux sociaux, etc.). Les personnes pourront saisir la Direction de l'Ethique et Données personnelles via la plateforme dans le cas où elles se sentiraient victimes de représailles afin de le signaler.

L'irresponsabilité pénale est garantie au lanceur d'alerte qui soustrait, détourne ou recèle des documents confidentiels contenant des informations liées à l'alerte, à condition qu'il en a eu accès de façon licite. Ces dispositions s'appliquent également au complice de ces infractions. Une irresponsabilité civile du lanceur d'alerte est également consacrée pour les préjudices pouvant découler de son alerte effectuée de bonne foi.
Lorsqu'un signalement ou une divulgation publique a été réalisé de manière anonyme, le lanceur d'alerte si son identité est révélée par la suite bénéficie des mêmes protections.

3.2. Protection des personnes visées par une alerte

Toutes les précautions sont également prises par les acteurs du dispositif d'alerte en vue de garantir la stricte confidentialité des éléments de nature à identifier les personnes visées par une alerte (identité, fonctions, coordonnées).

Il est rappelé que l'identité de la personne mise en cause par une alerte ne peut être divulguée, sauf à l'autorité judiciaire, qu'une fois établi le caractère fondé de l'alerte.

En toutes hypothèses, les éléments de nature à identifier la personne à l'origine de l'alerte ne sont jamais communiqués à la personne visée.

3.3. Protection des témoins

Toutes les précautions sont également prises par les acteurs du dispositif d'alerte en vue de garantir la stricte confidentialité des personnes qui témoignent. Les éléments de nature à identifier la personne à l'origine de l'alerte ne leur sont jamais communiqués.

3.4. Traitement des données à caractère personnel

Le dispositif de signalement et de traitement des alertes professionnelles décrit dans cette charte implique des traitements de données à caractère personnel pour lesquels Aéroports de Paris agit en tant que responsable de traitement.

Finalités et bases légales

Ces traitements ont pour finalité de permettre la réception et le traitement des questions et alertes reçues. Ils sont basés sur les obligations légales imposées à Aéroports de Paris (ADP SA) et aux entités constituant le Groupe ADP. Les données collectées et conservées sont hébergées de façon sécurisée conformément à la PSSI (Politique de Sécurité du Système d'Information) sur des espaces à accès restreint et seules les personnes habilitées peuvent en connaître. Le système d'alerte est inscrit dans le registre des activités de traitement d'ADP SA et une Analyse d'Impact relative à la Protection des Données personnelles (AIPD) a été réalisée.

Données collectées et traitées

Il est rappelé aux auteurs d'alertes qu'ils ne doivent communiquer dans le cadre du dispositif d'alerte que des informations factuelles présentant un lien direct avec l'objet de leur alerte.

Sont traitées dans le cadre du dispositif d'alerte, les données à caractère personnel suivantes :

- Identité, fonctions et coordonnées de la personne à l'origine de l'alerte lorsqu'elles sont communiquées (lanceur d'alerte et facilitateurs).
- Identité, fonctions et coordonnées de la personne visée par l'alerte lorsqu'elles sont communiquées.
- Identité, fonctions et coordonnées des parties prenantes au recueil et au traitement de l'alerte, notamment des témoins lorsqu'elles sont communiquées.
- Faits signalés.
- Éléments recueillis dans le cadre de la vérification des faits signalés.
- Comptes rendus d'entretiens et des opérations d'enquête / vérification.
- Suites données aux alertes.

Durée de conservation des données

Lorsque l'alerte est déclarée irrecevable, ces données sont archivées dans un délai de deux mois après anonymisation sous la responsabilité de la Direction de l'Ethique et Données personnelles.

Lorsque l'alerte est recevable

Pendant la durée de l'instruction, les données sont anonymisées à l'exception des pièces récoltées dans le cadre de l'instruction et sont conservées sur un lieu sécurisé où seules les personnes de la Direction de l'Ethique et Données personnelles désignées en annexe de la présente Charte ont accès.

Après clôture de l'instruction (vérifications ou enquêtes)

Tous les éléments récoltés et non annexés au rapport/document de vérification seront détruits deux mois après la clôture. Les pièces anonymisées et à conserver seront archivées deux mois après la clôture sur la plateforme d'alerte et sur le lieu sécurisé où où seules les personnes de la Direction de l'Ethique et Données personnelles désignées en annexe de la présente Charte ont accès.

Le rapport/document de vérification anonymisés et les pièces non anonymisées qui constituent l'annexe seront archivés dans le système d'archive C@pe d'Aéroports de Paris au plus tard deux mois après la clôture de l'enquête. Afin de pouvoir répondre à l'obligation de justifier du traitement des alertes, les documents archivés à la clôture sont conservés pour une durée de 12 ans.

Destinataires et transferts des données

Seules les personnes de la Direction de l'Ethique et Données personnelles désignées en annexe de la présente Charte ont accès aux données conservées sur un lieu sécurisé.

Les données à caractère personnel peuvent être communiquées à des tiers (par exemple, cabinet forensic, cabinets d'avocats) lorsque cela s'avère nécessaire au traitement de l'alerte (réception des alertes, enquête, expertise juridique). Ces prestataires signent avec Aéroports de Paris SA des contrats dans lesquels ils s'engagent à prendre des garanties suffisantes concernant le traitement et la sécurité des données qui leur sont confiées.

Dans le cas où des données à caractère personnel sont susceptibles d'être transférées en dehors de l'Espace Economique Européen, Aéroports de Paris SA met en place des garanties permettant d'assurer un niveau de protection suffisant des données, notamment via la signature des clauses contractuelles types de la Commission européenne (dont une copie est disponible sur demande à informatique.libertes@adp.fr).

Droits des personnes

Toute personne dont les informations sont exploitées dans le cadre de l'alerte, y compris des personnes visées par l'alerte, sont informées dans **un délai d'un mois** à compter de l'utilisation des données ou **dans un délai raisonnable** lorsqu'une telle information est susceptible de compromettre les nécessités de l'enquête (par exemple en présence d'un risque de destruction de preuves). Dans ce cas, cette information sera reportée et délivrée aussitôt le risque pour l'enquête écarté. Si des mesures conservatoires doivent être prises, le comité de traitement arbitrera la proportionnalité et la nécessité de telles mesures.

Conformément à la législation applicable en matière de Données personnelles, les personnes identifiées dans le cadre du dispositif d'alerte disposent d'un certain nombre de droits concernant la collecte et le traitement de leurs données à caractère personnel, à savoir :

- Le droit d'accès : les personnes ont le droit d'obtenir (i) la confirmation que des données à caractère personnel les concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, d'obtenir (ii) l'accès auxdites données et une copie de ces dernières. L'exercice de ce droit ne doit néanmoins pas porter atteinte aux droits et libertés des tiers ou empêcher le bon déroulement de l'enquête.
- Le droit d'opposition : lorsque le traitement est mis en œuvre pour permettre à Aéroports de Paris SA de se conformer à une obligation légale (loi Sapin II par exemple) alors le droit d'opposition n'est pas applicable.
- Le droit de rectification : les personnes ont le droit d'obtenir la rectification des données à caractère personnel les concernant qui sont inexactes. Elles ont également le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris en fournissant une déclaration complémentaire. Ce droit ne doit néanmoins pas permettre à la personne concernée de modifier rétroactivement des éléments contenus dans l'alerte ou collectées lors de son instruction.
- Le droit à la limitation du traitement : dans certains cas, les personnes ont le droit d'obtenir la limitation du traitement de leurs données à caractère personnel.
- Le droit de transmettre des instructions concernant l'utilisation des données après le décès : les personnes peuvent donner à Aéroports de Paris SA des directives concernant l'utilisation de leurs données à caractère personnel après leur décès.

Ces droits peuvent être exercés auprès de la Direction de l'Ethique et Données personnelles ou du délégué à la protection des données par courriel à : informatique.libertes@adp.fr ou par courrier à : délégué à la protection des données (1 rue de France, BP 81007, 95931 Roissy Charles de Gaulle Cedex).

Si les personnes concernées estiment, après avoir contacté le délégué à la protection des données, que leurs droits ne sont pas respectés, elles peuvent adresser une réclamation auprès de l'autorité de protection des données personnelles

4/ Modalités de traitement de l'alerte

4.1. Comment est-il accusé réception d'une alerte ?

Un accusé de réception permet d'informer la personne à l'origine de l'alerte qu'elle est bien parvenue à la Direction de l'Éthique et Données personnelles.

Il est envoyé automatiquement via la plateforme (si l'alerte y est déposée) ou sous 7 jours ouvrés par la Direction de l'Éthique et Données personnelles par e-mail et informe la personne à l'origine de l'alerte que sa recevabilité va faire l'objet d'un examen selon la procédure décrite ci-dessous.

Si le lanceur d'alerte le demande, une visio-conférence ou une rencontre physique peut être organisée pour soumettre le signalement. Dans ce cas, elle doit être organisée au plus tard 20 jours ouvrés après réception de la demande. Le signalement oral doit être correctement consigné (i.e., enregistrement, transcription ou procès-verbal). De même, le lanceur d'alerte doit avoir la possibilité de vérifier, de rectifier et d'approuver la transcription ou le procès-verbal avec une traçabilité de la rectification et/ ou de la validation.

4.2. Comment s'effectue l'examen de recevabilité d'une alerte ?

A la réception d'une alerte, la Direction de l'Ethique et de Protection des données effectue une analyse préliminaire afin d'apprécier sa recevabilité. Cette analyse préliminaire vise à déterminer si le signalement entre dans le champ d'application du dispositif, à savoir :

- Les personnes à l'origine de l'alerte répondent aux critères d'éligibilité.
- Les allégations entrent dans au moins un des champs d'application prévus par le dispositif.
- Dans certains cas, la Direction de l'Ethique et de Protection des données demande des informations complémentaires soit pour mieux comprendre le périmètre d'une alerte, soit pour pouvoir juger plus pertinemment de la recevabilité de l'alerte. Dans ce dernier cas, en l'absence de réponse du lanceur d'alerte, celle-ci sera jugée comme irrecevable. La vraisemblance des faits reportés.
- Le caractère circonstancié des faits reportés ou les éléments de preuve apportés.
- Le respect des principes définis dans la présente charte.

La direction de l'Ethique et protection des données pourra décider de mesures conservatoires avant même la constitution du comité de traitement si elle le juge nécessaire.

4.3. Comment est signifiée la recevabilité d'une alerte ?

Dans un délai **n'excédant pas trois mois** à compter de l'envoi de l'accusé de réception de l'alerte (ou à défaut, 3 mois à compter de l'expiration d'une période de 7 jours ouvrés suivant le signalement), la Direction de l'Ethique et Données personnelles informera la personne à l'origine de l'alerte de sa recevabilité dans le cadre du dispositif tel que décrit dans la présente charte. Cette information se fera par écrit et précisera les mesures envisagées ou prises pour évaluer l'exactitude des allégations et, le cas échéant, remédier à l'objet du signalement ainsi que sur les motifs de ces dernières.

En cas d'irrecevabilité, la Direction de l'Ethique et Données personnelles informera l'auteur des motifs de cette décision négative et lui indiquera les suites données à son signalement (clôture de l'alerte, transmission à un autre département pour traitement, etc.).

5/ Procédure de traitement des alertes recevables

5.1. Constitution d'un comité ad hoc

Une fois l'alerte déclarée comme recevable, la Direction de l'Ethique et Données personnelles analyse les informations recueillies pour identifier les différentes catégories d'allégations. Elle peut demander des informations complémentaires si besoin auprès de la personne à l'origine de l'alerte ou procéder à des vérifications liminaires qui permettront au comité de traitement d'éclairer sa décision sur la nature du traitement à apporter :

- Identification des éventuels traitements précédents ou parallèles. Par exemple, des actions déjà mises en œuvre par le réseau RH dans le cadre d'un mal-être au travail. Dans ce cas, la Direction de l'Éthique et des Données Personnelles pourra arbitrer sur la nécessité de suivre le traitement initié par l'autre département ou en mener un en parallèle,
- Description circonstanciée des faits, identités des personnes concernées,
- Identification des risques éventuels, potentiels conflits d'intérêts.
- Etc.

La Direction de l'Éthique et Données Personnelles composera un Comité de traitement ad hoc réunissant un nombre limité de personnes compétentes au regard du sujet traité (finance, juridique, RH, etc.), qui instruira les faits objets de l'alerte.

Lors de la première réunion, le comité de traitement réalisera une vérification formelle des potentiels conflits d'intérêts. Chaque membre s'engagera à ne pas en avoir. En cas de déclaration, les autres membres du comité préciseront comment ils souhaitent le traiter. Cette vérification s'inscrit en complément des diligences effectuées en amont par la Direction de l'Éthique et des Données Personnnelles lors de l'analyse de l'alerte.

Le Comité se réunit autant que nécessaire notamment pour valider la stratégie de traitement, pour piloter le déroulement du traitement de l'alerte, pour arbitrer, et pour valider les conclusions et recommandations s'il y a lieu. Le comité de traitement pourra également décider de mesures conservatoires.

5.2. Modalités de traitement de l'alerte recevable

Selon la nature, la gravité des faits signalés, ou les risques encourus, le Comité de traitement ad hoc pourra décider de la nature du traitement qui peut revêtir plusieurs formes.

Des vérifications pourront être menées par la Direction de l'Ethique et Données Personnelles, le Référent Ethique et Compliance, l'équipe d'enquête interne ou toutes autres personnes désignées par le Comité de traitement. Ces vérifications pourront soit permettre d'infirmer ou confirmer les allégations, soit serviront d'éléments pour alimenter d'autres modalités de traitement de l'alerte.

Un audit interne ou externe ou une mise sous monitoring d'audit existant.

Une enquête interne pouvant être menée par l'équipe d'enquête interne du Groupe ADP, ou autres (cabinet forensic, Référents de filiales, etc.), ou en combinant les solutions. Le comité de traitement choisira la solution la plus adaptée à l'alerte en tenant compte de plusieurs paramètres (indépendance, expertises particulières, périmètre de l'enquête, etc.).

Si le Comité diligente une enquête, son premier compte-rendu constituera l'ordre de mission de l'équipe d'enquête (lorsqu'il est fait appel à des cabinets extérieurs, l'appel d'offre remporté par le prestataire constituera l'ordre de mission).

Ou **toute autre action pertinente** décidée par le Comité de traitement.

5.3. Clôture de la procédure de traitement de l'alerte

La clôture de l'ensemble des opérations liées au traitement de l'alerte est décidée par le comité de traitement ad hoc.

La personne à l'origine de l'alerte et la personne visée par celle-ci sont informées par écrit par la Direction de l'Ethique et Données personnelles de la clôture de la procédure de traitement de l'alerte. A l'issue de l'enquête ou de vérifications, la Direction de l'Ethique et Données Personnelles pourra émettre des recommandations en se basant sur les conclusions de l'enquête et l'avis du Comité de traitement ad hoc. Ces recommandations pourront porter sur le cas ou sur le fonctionnement du Groupe (procédures, process…).

Le document formalisant les recommandations émises par la Direction de l'Ethique et Protection des données est remis aux personnes pertinentes et devant prendre les décisions attenantes à ces recommandations conformément à l'avis du comité de traitement. La transmission de ces recommandations matérialise la fin de l'enquête et donc la clôture de la procédure.

En cas de recommandation d'une sanction disciplinaire, le délai pour engager la procédure de sanction débute à compter de la connaissance des faits fautifs par la personne habilitée à la déclencher (c'est-à-dire à la date d'envoi du document contenant les recommandations).

5.4. Le suivi du dispositif

Chaque année, la Direction de l'Ethique et Données personnelles réalise un rapport des actions menées au Comité d'Audit et des risques, au Conseil d'Administration ainsi qu'au COMEX. Dans ce cadre, il sera fait un point sur le dispositif d'alerte via un tableau de suivi statistique qui contient des informations anonymisées sans données à caractère personnel et ne permettant pas de faire le rapprochement avec un collaborateur afin de protéger son identité.

Ces actions peuvent conduire à la mise à jour ou à la révision anticipée des éléments suivants :

- la cartographie des risques de corruption,
- le Code de conduite,
- le plan de Formation,
- les procédures éthique et compliance
- les procédures concernant le traitement des alertes internes,
- les procédures de contrôle interne (contrôles comptables, contrôles Ethique…),
- le régime disciplinaire.

6/ L'enquête interne

6.1. Les principes de l'enquête interne

Les enquêtes, qu'elles soient menées en interne ou en externe, sont soumises aux règles contenues dans le document relatif à la déontologie de l'enquête interne et aux principes fondamentaux suivants :

- Le professionnalisme.
- Le respect de la confidentialité.
- La neutralité / l'impartialité.
- L'objectivité.
- Le respect de la présomption d'innocence.
- Par mesures conservatoires, la direction de l'Ethique et Données personnelles pourra différer l'information faite au manager et au collaborateur mis en cause par l'alerte dès lors que le comité de traitement le valide.

Les alertes signalant des cas de mal-être ou de harcèlement sont traitées au même titre que les autres alertes mais certaines précautions sont prises compte tenu des risques psychosociaux importants pouvant en découler.

En outre, si **l'alerte présente des risques psychosociaux avérés ou pressentis**, la Direction de l'Ethique et Données Personnelles alerte les personnes ou entités concernées du Groupe (médecin du travail, responsable en charge de la qualité de vie au travail, etc.) directement ou via la personne jugée la plus à même d'effectuer cette alerte (manager, par exemple) afin que ce risque soit pris en charge tout en poursuivant le traitement du signalement reçu.

La Direction de l'Ethique et Données personnelles pourra prendre les mesures conservatoires nécessaires, (sans présumer des responsabilités de chacune des parties) en collaboration avec la Direction des Ressources Humaines afin de protéger le lanceur d'alerte et/ou la personne visée par l'alerte.

DANS TOUS LES CAS :

La Direction de **l'Éthique et Données personnelles reste responsable du traitement de l'alerte et garde la relation privilégiée avec la personne à l'origine de l'alerte.**

Si les enquêtes ou audits menés à la suite d'une alerte peuvent avoir de fortes implications professionnelles et personnelles pour les personnes mises en cause, ces investigations ne **sauraient toutefois en aucun cas s'apparenter à une enquête judiciaire.** Le comité ad hoc pourra en fin d'instruction, dans l'hypothèse où l'alerte aurait démontré l'existence d'une infraction pénale, transmettre le dossier aux autorités judiciaires afin que celles-ci y donnent suite.

6.2. Coopération des salariés entendus dans le cadre d'une enquête

En vertu de l'obligation de loyauté inhérente à leur contrat de travail, les salariés entendus dans le cadre d'une enquête sont tenus de coopérer au bon déroulement de celle-ci. À ce titre, il est notamment attendu d'eux :

- qu'ils signent l'engagement de confidentialité qui leur est communiqué,
- qu'ils se présentent aux entretiens sollicités par l'équipe d'enquête,
- qu'ils répondent de bonne foi aux questions posées par l'équipe d'enquête,
- qu'ils communiquent tout élément utile aux investigations demandé par l'équipe d'enquête.

Tout comportement ou agissement susceptible d'entraver les investigations, notamment en refusant de se rendre aux entretiens ou de répondre aux questions de l'équipe d'enquête, en trompant, ou en dissimulant des informations, est susceptible d'amener l'entreprise à en tirer toutes les conséquences de droit qui s'imposent.

7/ Annexes

Modalités de contrôle de l'utilisation du Système d'Information en cas de doute sur le respect des règles de déontologie et de bonne conduite pour la sécurité de l'information

Se reporter à la procédure interne (applicable uniquement à ADP SA) présente sur le site intranet : http://portail/sites/ethique_et_compliance ou sur demande auprès de la Direction de l'Ethique et Données personnelles du Groupe (stephanie.scouppe@adp.fr).

LE RÉSEAU ETHIQUE ET COMPLIANCE DU GROUPE ADP

Au niveau du Groupe ADP et chez Aéroports de Paris SA :		
Personnes en charge du pilotage du dispositif d'alerte	**Stéphanie SCOUPPE** Directrice de l'Éthique En son absence : **Isabelle CHIESA** Adjointe à la Directrice de l'Ethique	Mail : stephanie.scouppe@adp.fr Mail : isabelle.chiesa@adp.fr
	Nathalie VICTORY **Responsable du pôle Enquêtes** En son absence : **Arnaud NICOLAS** Enquêteur interne	Mail : nathalie.victory@adp.fr Mail : arnaud.nicolas@adp.fr
Les personnes listées sont également habilitées à accéder aux données collectées et traitées dans le cadre des alertes		

Chez Airport International Group (AIG) – Aéroport d'Amman – Jordanie	
Hazem KHIRFAN Director legal and compliance / Directeur Juridique et Compliance AIG	Mail : Hazem.Khirfan@aig.aero

Chez TAV Airports :	
Can ALPTEKIN Head of Audit	Mail : Can.Alptekin@tav.aero

Chez Hub One :	
Olivier MELLINA-GOTTARDO Secrétaire Général / Déontologue	Mail : olivier.mellina-gottardo@hubone.fr

Les 10 règles applicables au dispositif d'alerte

1) Le dispositif d'alerte est instauré en application de dispositions légales et règlementaires (les lois Sapin II et Potier) et le Code de conduite annexé au RI d'ADP SA et leurs équivalents dans les filiales.

2) L'utilisation du dispositif d'alerte n'est pas une obligation. C'est un droit que les personnes concernées exercent librement.

3) Les alertes peuvent être anonymes à condition que les éléments factuels signalés soient suffisamment détaillés et que la gravité des faits est établie ;

4) Une organisation spécifique est mise en place pour recueillir et traiter les alertes : les Référents Éthique et Compliance chargés du dispositif d'alerte sont astreints à une obligation de confidentialité renforcée notamment quant aux données dont ils prennent connaissance. Toute rupture de confidentialité est sanctionnée pénalement (jusqu'à 2 ans d'emprisonnement et 30 000 euros d'amende) ;

5) Les Référents Éthique et Compliance en charge du traitement de l'alerte en accusent réception dans un délai de sept jours à compter de sa réception et statuent sur sa recevabilité dans un délai maximum de trois mois ;

6) La personne à l'origine de l'alerte n'encourt aucune sanction du fait de l'utilisation de bonne foi et sans contrepartie financière directe de ce dispositif, son signalement restera confidentiel tout au long de son traitement, sauf accord préalable exprès ; les lanceurs d'alerte et facilitateurs sont protégés contre toutes représailles et peuvent contacter à tout moment la Direction de l'Ethique et Données personnelles directement ou via la plateforme.

7) Aucune personne ne peut, pour avoir signalé ou divulgué des informations, faire l'objet notamment des mesures suivantes, ni de menaces ou de tentatives de recourir à ces mesures : 1° Suspension, mise à pied, licenciement ou mesures équivalentes ; 2° Rétrogradation ou refus de promotion ; 3° Transfert de fonctions, changement de lieu de travail, réduction de salaire, modification des horaires de travail ; 4° Suspension de la formation ; 5° Évaluation de performance ou attestation de travail négative ; 6° Mesures disciplinaires imposées ou administrées, réprimande ou autre sanction, y compris une sanction financière ; 7° Coercition, intimidation, harcèlement ou ostracisme ; 8° Discrimination, traitement désavantageux ou injuste ; 9° Non-conversion d'un contrat de travail temporaire en un contrat permanent, lorsque le travailleur pouvait légitimement espérer se voir offrir un emploi permanent ; 10° Non-renouvellement ou résiliation anticipée d'un contrat de travail temporaire ; 11° Préjudice, y compris les atteintes à la réputation de la personne, en particulier sur les réseaux sociaux, ou pertes financières, y compris la perte d'activité et la perte de revenu ; 12° 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 au niveau du secteur ou de la branche d'activité ; 13° Résiliation anticipée ou annulation d'un contrat pour des biens ou des services ; 14° Annulation d'une licence ou d'un permis ; 15° Orientation vers un traitement psychiatrique ou médical.

8) Une alerte intentionnellement mensongère ou une alerte qui laisserait apparaître une collusion entre la personne l'émettant et la personne visée, pourrait être sanctionnée conformément au Règlement intérieur ;

9) Le dispositif d'alerte respecte les dispositions légales et règlementaires et est conforme à la loi informatique et libertés du 6 janvier 1978 et au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, Règlement Général sur la Protection des données (RGPD).

10) L'utilisateur du dispositif et toute personne visée par le dispositif bénéficient, dans les limites de la législation applicable, de plusieurs droits sur leurs données à caractère personnel (droit d'accès, de modification, de suppression, droit d'opposition, de limitation du traitement et de transmission de directives post-mortem) qu'ils peuvent exercer auprès de la direction de l'Ethique et Données personnelles.

isabelle.chiesa@adp.fr
ou stephanie.scouppe@adp.fr

ou du délégué à la protection des données :
Par courriel :
informatique.libertes@adp.fr

par courrier :
1 rue de France BP 81007
95931 Roissy Charles de Gaulle Cedex

Déontologie de l'enquête interne

Conformément à la Charte pour le traitement des alertes éthique et compliance, le Comité de traitement ad hoc constitué par la Direction de l'Ethique et Données personnelles peut décider de diligenter une enquête interne afin d'instruire l'alerte reçue dans le cadre du dispositif mis en place par le Groupe ADP.

Le présent document a pour objectif de formuler les principes généraux régissant les enquêtes internes et applicables aux personnes désignées par le Comité de Traitement ad hoc afin de les mener, ainsi que de détailler le déroulement de ces enquêtes.

Les règles contenues dans ce document s'appliqueront également aux enquêteurs ou auditeurs tiers désignés par la Direction de l'Ethique et Données personnelles après avis du Comité de traitement.

Principes généraux régissant les enquêtes internes

Article I

L'enquête interne diligentée afin d'instruire une alerte ne saurait s'apparenter à une enquête judiciaire. Les personnes en charge de l'enquête interne agissent dans le strict respect des lois et règlements en vigueur ainsi que des règles de l'entreprise, dont ils se tiennent informés.

Article II

L'enquête interne porte sur des faits délictueux ou présumés comme tels ou une violation du règlement intérieur, ou équivalent, ou du code de conduite, révélés par l'alerte et non sur des personnes.

Elle a pour but de vérifier la matérialité des faits objet de l'alerte, le cas échéant, d'en identifier les auteurs présumés et de collecter les éléments nécessaires pour engager une procédure disciplinaire et éventuellement judiciaire et recommander toute mesure d'amélioration des process du groupe.

Article III

Dans leurs investigations et dans la restitution de leurs travaux, les personnes en charge de l'enquête interne doivent respecter les principes suivants : intégrité, objectivité, neutralité, impartialité, confidentialité et respect du principe du contradictoire.

Les personnes en charge de l'enquête interne devront, le cas échéant, se retirer dès lors qu'ils estiment être en conflit d'intérêts soit du fait de leur relation particulière avec l'une des personnes sur laquelle peut porter l'enquête, soit de leur implication sur le projet en cause.

Article IV

L'enquête interne est menée dans le respect de la vie privée et des droits de la personne.

L'enquêteur s'interdit d'utiliser ou de divulguer, directement ou indirectement toute information recueillie dans le cadre de ses activités, en dehors du cadre de l'enquête.

L'enquêteur interne ne recherche, ni ne divulgue des éléments touchant à la situation personnelle, familiale ou médicale d'un collaborateur, sauf si cela est rendu indispensable pour les conclusions de l'enquête.

Elle respecte la déclaration de ce traitement au registre des activités de traitement de données personnelles du Groupe.

Conduite d'une enquête interne

Article V

L'enquête interne est conduite à charge et à décharge, par au moins deux personnes, dans le strict respect de la présomption d'innocence des personnes concernées.

Les investigations sont menées sur la base de preuves factuelles et objectives en faisant abstraction de toute conviction, impression personnelle ou rumeur et de tout jugement de valeur.

Article VI

Les personnes en charge de l'enquête interne font état de leur qualité auprès des personnes rencontrées et/ou auditionnées (cf. infra).

En application de l'obligation de confidentialité renforcée qui leur incombe dans le cadre du traitement de l'alerte, elles ne sont pas tenues d'apporter de précisions sur les circonstances de leurs demandes.

Article VII

Les personnes en charge de l'enquête interne ont accès à l'ensemble des entités et des sites du Groupe ADP, ainsi qu'à toute information ou système d'information dont la consultation est nécessaire à la réalisation de la mission qui leur a été confiée, à l'exception des éléments relevant du secret de la défense nationale.

Pour l'accès aux systèmes d'informations la procédure et les modalités de saisie établies devront être strictement respectées. Ils peuvent demander copie de tous documents utiles à l'enquête.

Article VIII

En tant que de besoin, les personnes chargées de l'enquête interne peuvent procéder à l'audition de personnes (témoins, personnes visées par l'alerte, toute autre personne utile) pour recueillir leurs explications sur les faits objet de l'alerte.

Ils peuvent avoir recours à un avocat « enquêteur », un « collecteur de preuves » pour qu'il diligente une investigation interne, soit dans une démarche en réponse à une alerte, soit alors même qu'une enquête sur l'existence potentielle de pratiques illicites en son sein et menée par une autorité administrative ou judiciaire est déjà ouverte.

Dans le cadre de ces auditions, aucune pression, menace ou intimidation à l'égard des personnes parties prenantes entendues ne saurait être exercée.

Les auditions s'opèrent par deux personnes et font systématiquement l'objet d'un compte-rendu rédigé par les personnes ayant mené l'audition et soumis à la validation de la personne entendue.

Article IX

L'ensemble des actions menées dans le cadre de l'enquête interne ayant permis de collecter des éléments de preuve doivent respecter des règles strictes destinées à assurer la protection des personnes.

Communication des constatations

Article X

Les constatations résultant de l'enquête interne font l'objet d'un rapport veillant à ne pas contenir d'éléments de nature à identifier la personne à l'origine de l'alerte.

Ce rapport devra être validé par le Comité de traitement ad hoc constitué par la direction Éthique et Données personnelles.

Si les résultats de l'enquête interne ont permis d'infirmer les faits objet de l'alerte, toutes les informations et données collectées devront être effacées conformément à la Charte pour le traitement des alertes éthique et compliance.