| CDC INFORMATIQUE | Date d'application 15/05/2026<br><br>Accès public | **Sous-domaine : Politique et stratégie de l'entreprise**<br>**Procédure relative au dispositif d'alerte professionnelle de CDC Informatique** |
|---|---|---|
| **Domaine : Pilotage** | Responsable de la procédure :<br>Direction de la Maitrise des Risques, du Contrôle permanent, de la Conformité et de la Déontologie de CDC Informatique (DMRCC ICDC) | **V1** |

# Procédure relative au dispositif d'alerte professionnelle de CDC Informatique

| | |
|---|---|
| Auteur | Direction de la Maitrise des Risques, du Contrôle permanent et de la Conformité de CDC Informatique (DMRCC ICDC) – Service Conformité et déontologie |
| Périmètre d'application | CDC Informatique |
| Description | Cette procédure a pour objet de préciser les modalités d'exercice du droit d'alerte au sein de CDC Informatique, en définissant notamment le circuit interne de recueil et de traitement des signalements. |
| Date d'effet | 15/05/2026 |
| Destinataires | - Toute direction et tout collaborateur de CDC Informatique<br>- Titulaires de droits de vote au sein de l'assemblée générale de CDC Informatique<br>- Membres de l'organe d'administration, de direction ou de surveillance<br>- Autres personnes bénéficiaires du droit d'alerte (anciens collaborateurs de CDC Informatique, candidats à un emploi au sein de CDC Informatique, collaborateurs extérieurs et occasionnels, prestataires, fournisseurs et sous-traitants) via une publication sur le site Internet de CDC Informatique |
| Validation de la version | Directrice de la Maitrise des Risques, du Contrôle permanent et de la Conformité de CDC Informatique (DMRCC ICDC),<br>Déontologue de CDC Informatique<br>Céline Cuillerdier |

| Version | Date de diffusion | Objet de la révision |
|---|---|---|
| V1 | 12/09/2025 | Création de la procédure |

*Le document est disponible sur l'intranet de CDC Informatique (https://caissedesdepots.sharepoint.com/sites/WeShare/SitePages/D%C3%89ONTOLOGIE.aspx) et sur le site internet de CDC Informatique : https://www.icdc.caissedesdepots.fr/*

*Pour toute question relative à la déontologie, le service Déontologie est joignable à l'adresse électronique suivante :* deontologie-icdc@caissedesdepots.fr

| CDC INFORMATIQUE | Date d'application 15/05/2026<br><br>Accès public | **Sous-domaine : Politique et stratégie de l'entreprise**<br>**Procédure relative au dispositif d'alerte professionnelle de CDC Informatique** |
|---|---|---|
| **Domaine : Pilotage** | Responsable de la procédure :<br>Direction de la Maitrise des Risques, du Contrôle permanent, de la Conformité et de la Déontologie de CDC Informatique (DMRCC ICDC) | **V1** |

**Sommaire**

## 1. Contexte et définitions

La présente procédure vise à préciser **les modalités d'exercice du droit d'alerte** prévu par le Code de déontologie de CDC Informatique et par la réglementation, en particulier par 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 »)** modifiée[1].

La présente procédure prend en considération les textes suivants :

- La loi n°2016-1691 du 9 décembre 2016 (dite « loi Sapin II ») relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique (dans ses articles 6 à 13 et 17 II) ;
- La loi n°2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte (loi de transposition de la directive européenne du 23 octobre 2019) ;
- Le décret n° 2022-1284 du 3 octobre 2022 relatif aux procédures de recueil et de traitement des signalements émis par les lanceurs d'alerte et fixant la liste des autorités externes (décret d'application de la loi du 21 mars 2022 abrogeant le décret n°2017-564 du 19 avril 2017) ;
- La délibération Cnil n° 2023-064 du 6 juillet 2023 portant abrogation de la délibération n° 2019-139 du 18 juillet 2019 portant adoption d'un référentiel relatif aux traitements de données à caractère personnel destinés à la mise en œuvre d'un dispositif d'alertes professionnelles et adoption d'un référentiel relatif aux traitements de données à caractère personnel destinés à la mise en œuvre d'un dispositif d'alertes professionnelles.

Le droit d'alerte offre la possibilité d'adresser un signalement directement au déontologue de CDC Informatique[2], fonction exercée en toute indépendance et impartialité par la Directrice de la Maitrise des Risques, du Contrôle permanent et de la Conformité de CDC Informatique (DMRCC) dans les conditions prévues par la présente procédure.

L'objectif principal est de garantir au lanceur d'alerte, ainsi qu'aux personnes physiques ou morales en lien avec lui (au sens de la définition rappelée au § 3.2.), une stricte confidentialité et un régime de protection renforcé, notamment contre toute forme de représailles.

L'instruction de ces alertes s'effectue dans le respect de la réglementation relative à la protection des données à caractère personnel et notamment l'obligation d'informer les personnes concernées des objectifs et finalités poursuivis par le dispositif d'alerte[3].

[1] La loi n°2016-1691 du 9 décembre 2016 a été modifiée par la loi n° 2022-401 du 21 mars 2022 (dite loi Wassermann) visant à améliorer la protection des lanceurs d'alerte, dont la mise en œuvre a été précisée par le décret n°2022-1284 du 3 octobre 2022.
[2] Le II de l'article 5 du décret du 3 octobre 2022 prévoit que le référent déontologue peut être chargé du recueil et, le cas échéant, du traitement des signalements
[3] Le recueil et le traitement de données dans le cadre de ce dispositif respectent les préconisations du référentiel relatif aux dispositifs d'alertes professionnelles (DAP) établi par la CNIL pour se conformer au RGPD

### 1.1. Dans quels cas recourir au dispositif d'alerte ?

Conformément à l'article 6 de la loi Sapin II, le dispositif d'alerte mis en place au sein de CDC Informatique peut être utilisé pour **signaler des informations portant sur** :

- **un crime ou un délit** (*tels que corruption, trafic d'influence, autres manquements à la probité, blanchiment d'argent, fraude, escroquerie, abus de biens sociaux, détournement d'actifs et vol*) ;
- **une menace ou un préjudice pour l'intérêt général** *(tels que des agissements susceptibles de faire courir un danger ou une atteinte à la sécurité de la population dans le domaine de la santé ou de l'environnement)* ;
- **une violation ou une tentative de dissimulation d'une violation d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement ou du droit de l'Union européenne** (*telle qu'une atteinte aux droits de l'homme et aux libertés fondamentales*) ;
- **une violation ou une tentative de dissimulation d'une violation de la loi ou du règlement**.

Seules les informations portant sur des situations illicites ou d'atteintes à l'intérêt général peuvent faire l'objet d'un signalement. Des dysfonctionnements mineurs au sein d'un service, n'entraînant pas de menace pour l'intérêt général et ne violant aucun texte, ne peuvent donc pas donner lieu à une alerte permettant de bénéficier du régime de protection prévu par la loi Sapin II.

**Exclusion du champ de l'alerte**

Sont exclus du régime du droit d'alerte les faits, informations et documents couverts par le secret de la défense nationale, le secret médical, le secret des délibérations judiciaires, le secret de l'enquête ou de l'instruction judiciaires ou le secret professionnel de l'avocat.

### 1.2. Qui peut avoir recours au dispositif d'alerte ?

Les personnes pouvant émettre un signalement sont les personnes répondant à la définition de « lanceur d'alerte » tel qu'énoncée à l'article 6 de la loi n° 2016-1691 dite Sapin II du 9 décembre 2016 tel que modifiée par la loi du 21 mars 2022.

Ainsi, **le lanceur d'alerte est une personne physique** :

- qui signale ou divulgue, sans contrepartie financière directe et de bonne foi, des informations portant sur un crime, un délit, une menace ou un préjudice pour l'intérêt général, une violation ou une tentative de dissimulation d'une violation d'un engagement international régulièrement ratifié

ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, du droit de l'Union européenne, de la loi ou du règlement.

- qui a obtenu ces informations dans le cadre des activités professionnelles ou qui en a eu personnellement connaissance.

Par conséquent, conformément à l'article 8 de la loi Sapin II, il peut s'agir de toute personne physique telle que :

- **Les membres du personnel**[4], **les personnes dont la relation de travail s'est terminée**, lorsque les informations ont été obtenues dans le cadre de cette relation, et **les personnes qui se sont portées candidates à un emploi au sein de CDC Informatique**, lorsque les informations ont été obtenues dans le cadre de cette candidature ;

- **Les titulaires de droits de vote au sein de l'assemblée générale de CDC Informatique** ;

- **Les membres de l'organe d'administration, de direction ou de surveillance** ;

- **Les collaborateurs extérieurs et occasionnels**[5] ;

- **Les cocontractants de CDC Informatique**[6], 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 cocontractants et sous-traitants ainsi que les membres de leur personnel.

### 1.3. Quelles sont les conditions pour émettre une alerte ?

Conformément à l'article 6 de la loi Sapin II, outre le respect du cadre défini aux § 1.1. et 1.2, les conditions suivantes sont requises pour que l'auteur du signalement puisse être qualifié de lanceur d'alerte et bénéficier des mesures de protection afférentes à ce statut :

- **Absence de contrepartie financière directe** : le lanceur d'alerte ne peut solliciter ou percevoir de rémunération en contrepartie de l'alerte qu'il émet.

- **Exercice de bonne foi**[7] : le lanceur d'alerte doit agir de bonne foi avec, selon les termes de la règlementation, « *des motifs raisonnables de croire que les informations signalées étaient véridiques*

[4] Les membres du personnel sont ci-après désignés sous le terme « collaborateurs », dans la présente procédure, et couvrent tous salariés de CDC Informatique, y compris les alternants.
[5] Il s'agit notamment des intérimaires ou encore des stagiaires.
[6] Il s'agit notamment des prestataires de service ayant un contrat en cours avec CDC Informatique ainsi que leurs salariés, des fournisseurs de CDC Informatique, des partenaires liés par un contrat, etc.
[7] La bonne foi repose notamment sur la légitimité du but poursuivi, l'absence d'animosité personnelle, la prudence dans l'expression (Cass. civ. 1re, 28 sept. 2016, n° 15-21823 et Conseil d'État CE, 8 déc. 2023, n° 435266). Ainsi, la bonne foi n'exige pas que les faits dénoncés soient ultérieurement établis, mais qu'ils aient été rapportés avec honnêteté et loyauté, sans intention malveillante ni volonté de nuire.

*au moment du signalement* »[8] . Cette exigence est une garantie essentielle contre les signalements malveillants, fantaisistes ou abusifs, dès lors qu'elle garantit que les informations erronées ou trompeuses ne se voient pas accorder de protection.

Ainsi, l'utilisation de bonne foi du dispositif, même si les faits ne s'avèrent pas fondés ou ne donnent lieu à aucune suite, n'expose son auteur à aucune sanction. A contrario, l'utilisation abusive du dispositif, par le signalement d'informations qu'il sait erronées ou trompeuses, peut exposer l'agent à des sanctions disciplinaires ainsi qu'à des poursuites judiciaires.

- **Connaissance des faits signalés dans un cadre professionnel** : le signalement concerne des informations obtenues par le lanceur d'alerte dans le cadre de ses activités professionnelles et portant sur des faits qui se sont produits ou sont très susceptibles de se produire au sein de CDC Informatique. Il peut aussi signaler ces faits dès lors qu'ils lui ont été rapportés par un tiers, y compris en dehors du cadre professionnel, et qu'ils lui paraissent véridiques. Lorsque les informations n'ont pas été obtenues dans le cadre des activités professionnelles, le lanceur d'alerte doit en avoir eu personnellement connaissance.

Sans préjudice des obligations prévues par les textes (notamment l'article 40 du code de procédure pénale cf. § 2.2.), **l'exercice du droit d'alerte est laissé à l'appréciation personnelle de chacun** : il est facultatif et aucune sanction disciplinaire ne saurait être prise contre une personne au motif qu'elle n'aurait pas émis d'alerte.

## 2. Circuits de recueil et de traitement des alertes

La personne souhaitant émettre une alerte peut choisir entre différents canaux :

- soit utiliser le **dispositif d'alerte interne** mis en place au sein de CDC Informatique (Cf § 2.1.) ;
- soit adresser une **alerte externe**, après avoir effectué ou non une alerte interne (Cf § 2.2.).

Le lanceur d'alerte peut en outre procéder à une divulgation publique sous certaines conditions (§ Cf 2.3.).

### 2.1. Quel dispositif d'alerte interne est mis en place à CDC Informatique ?

CDC Informatique met en place un dispositif interne et centralisé de recueil et de traitement des signalements permettant de prendre en charge avec diligence toutes les alertes définies au § 1.1.

#### *2.1.1. Comment émettre une alerte en interne ?*

[8] 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.

Les personnes pouvant émettre une alerte (telles que définies au § 1.2.) peuvent adresser leur signalement par écrit par l'un quelconque des moyens suivants :

- **par courrier électronique à l'adresse dédiée suivante : deontologie-icdc@caissedesdepots.fr** ;
- **par courrier recommandé avec demande d'avis de réception à l'adresse suivante : CDC Informatique, à l'attention de la Déontologue de CDC Informatique (DMRCC) 18 avenue Aristide Briand, 92220 Bagneux.**

Il est recommandé que l'envoi postal soit effectué sous double enveloppe : une enveloppe intérieure comprenant les éléments de l'alerte, sur laquelle figure la mention « signalement d'une alerte », la mention « confidentiel » et la date de l'alerte et une enveloppe extérieure adressée au déontologue.

### ➢ Quelles informations doivent être communiquées par le lanceur d'alerte ?

Le signalement doit expliquer de façon la plus étayée et documentée possible les motifs de l'alerte, sans oublier de mentionner les dates des faits relatés. Il doit être fondé sur des faits et non sur de simples rumeurs.

Seul le lanceur d'alerte détermine la nature et le volume des informations, notamment à caractère personnel, communiquées à l'occasion de son alerte. Néanmoins, il doit veiller à ne transmettre que des informations factuelles et présentant un lien direct avec l'objet de l'alerte[9].

Un formulaire de signalement d'une alerte facultatif est mis à disposition par CDC Informatique sur son intranet et sur la page d'accueil de son site internet « icdc.caissedesdepots.fr », et figure en annexe à la présente procédure.

### ➢ Pourquoi le lanceur d'alerte a-t-il intérêt à donner son identité ?

Les garanties de protection qui encadrent ce dispositif ne peuvent être mises en œuvre que si l'identité de la personne exerçant son droit d'alerte est précisée (ou connue par le déontologue).

Si l'auteur de l'alerte n'est pas un collaborateur de CDC Informatique, il doit transmettre en même temps que son alerte les éléments permettant de justifier qu'il appartient à l'une des catégories de bénéficiaires du droit d'alerte mentionnées au §1.2. (notamment s'il s'agit d'un candidat à un emploi ou d'un collaborateur d'un prestataire).

Une alerte par une personne qui souhaite rester anonyme ne sera traitée que si les éléments rapportés sont suffisamment factuels, détaillés et sérieux. Le traitement des alertes anonymes s'entourera de

[9] Recommandations de la CNIL (Référentiel relatif aux traitements des données à caractère personnel destinés à la mise en œuvre d'un dispositif d'alertes professionnelles, 6 juillet 2023)

précautions particulières, impliquant un examen approfondi de l'opportunité d'y répondre. Ces alertes, tant qu'elles restent anonymes, ne garantissent pas à leur auteur le statut protecteur de lanceur d'alerte tel que précisé au § 3[10].

➢ **Qui est destinataire de l'alerte ?**

Les destinataires de l'alerte sont :

- Le déontologue de CDC Informatique, Directeur-trice de la Maitrise des Risques, du Contrôle permanent et de la Conformité de CDC Informatique (DMRCC) ;
- Les autres personnes composant le service Déontologie.

Conformément à l'article 6 du décret n°2022-1284 du 3 octobre 2022, les signalements reçus par d'autres personnes ou services au titre de la présente procédure doivent être transmis sans délai aux personnes mentionnées ci-dessus selon les modalités décrites au § 2.1.1.

➢ **Qui est destinataire de l'alerte lorsque celle-ci porte sur la déontologue ou son équipe** ?

Dans ce cas, l'auteur de l'alerte doit procéder au signalement auprès du directeur général de CDC Informatique.

Le signalement doit être adressé par écrit par l'un quelconque des moyens suivants :

- **par courrier électronique à l'adresse dédiée : mathias.guerin@caissedesdepots.fr** ;
- **par courrier recommandé avec demande d'avis de réception à l'adresse suivante : CDC Informatique, à l'attention du Directeur général de CDC Informatique 18 avenue Aristide Briand, 92220 Bagneux.**

Il est recommandé que l'envoi postal soit effectué sous double enveloppe : une enveloppe intérieure comprenant les éléments de l'alerte, sur laquelle figure la mention « signalement d'une alerte », la mention « confidentiel » et la date de l'alerte et une enveloppe extérieure adressée au Directeur général de CDC Informatique.

L'alerte est traitée selon les modalités décrites dans la présente procédure par le Directeur Général de CDC Informatique garantissant la confidentialité.

En particulier,

[10] Le lanceur d'alerte dont l'identité a été révélée ultérieurement bénéficie alors des garanties de protection

- Le traitement de l'alerte et les échanges avec le lanceur d'alerte et toute personne visée par l'alerte sont effectués au moyen d'une **adresse électronique dont l'accès est restreint** au Directeur Général,
- Tout document et toute information sont **stockés sur un répertoire protégé, dédié et sécurisé** auquel seul le Directeur Général a accès, tout accès d'une personne non habilitée faisant l'objet d'une détection et d'une vérification de sécurité.

### *2.1.2. Comment est traitée l'alerte ?*

Sauf à ce que l'alerte porte sur le déontologue et/ou une personne de son équipe), la gestion du dispositif d'alerte est assurée par le déontologue appuyé par les personnes de son équipe telles que mentionnées ci-dessus dûment habilitées par lui et astreintes à une obligation renforcée de confidentialité.

Le déontologue est par ailleurs **garant de l'indépendance et de l'impartialité** des missions liées au traitement de l'alerte, notamment en s'assurant que lui-même et les personnes de son équipe chargées de l'instruction du dossier ne se trouvent pas en situation de conflits d'intérêts au regard de l'auteur de l'alerte ou des tiers concernés par l'alerte.

Dans le respect des garanties rappelées ci-dessus, le déontologue et les personnes de son équipe chargées du traitement des alertes peuvent :

- **demander tout complément d'information à l'auteur de l'alerte**. . Pour les alertes reçues par courrier postal, tous les échanges, ainsi que la transmission des informations ou documents complémentaires se font via courrier postal, sauf si l'auteur du signalement a précisé une adresse électronique dans son courrier. Dans ce cas, les échanges se feront par courriel ;
- **s'appuyer sur d'autres expertises** (principalement de la Direction des ressources humaines) et, le cas échéant, celle du Déontologue de la Caisse des Dépôts. Par ailleurs, si une enquête interne s'avère nécessaire, le déontologue peut s'adresser à l'Inspecteur général, directeur de l'audit du Groupe, qui dispose de prérogatives particulières pour mener des investigations, ou faire appel à un prestataire externe et/ou à un cabinet d'avocats. Le déontologue peut également inviter temporairement d'autres contributeurs pour le traitement des alertes[11].
- A noter que tous les prestataires externes susceptibles d'intervenir dans le cadre du traitement d'une alerte sont soumis à une obligation de confidentialité renforcée par la signature d'un engagement de confidentialité leur rappelant leurs obligations et les sanctions associées**.**

➢ **Réception de l'alerte**

[11] Toute personne sollicitée dans le cadre de l'instruction doit être notifiée formellement des obligations de confidentialité qui s'imposent à elle et doit en accuser réception par écrit.

Le déontologue **accuse réception, par écrit, de l'alerte dans les 7 jours ouvrés** suivant sa réception.

### ➢ Recevabilité de l'alerte

Le déontologue **effectue un examen préalable de l'alerte afin d'en évaluer la recevabilité** au regard de son objet, de l'identité de son auteur (si l'alerte n'est pas anonyme) et de ses conditions d'exercice (bonne foi, absence de contrepartie financière directe, connaissance des informations)[12].

Des informations complémentaires peuvent, si nécessaire, être demandées à l'auteur de l'alerte pour en examiner sa recevabilité. Une alerte peut être jugée non recevable en l'absence de communication par son auteur d'éléments factuels suffisamment détaillés permettant son traitement.

Il informe l'auteur du signalement de la **recevabilité de l'alerte dans un délai d'un mois** à compter de l'accusé de réception.

En cas de non-recevabilité, le déontologue en communique les raisons à l'auteur du signalement et procède à la clôture du dossier au titre de l'alerte. Dans ce cas l'auteur du signalement ne bénéficie pas de la protection.

L'alerte est clôturée notamment dans le cas où les faits ont déjà fait l'objet d'une **procédure juridictionnelle ou disciplinaire, en cours ou ayant donné lieu à une décision**, ou lorsqu'il s'agit d'alertes :

- ayant donné lieu à une saisine, en cours ou ayant abouti, de **l'inspection du travail ou du Défenseur des droits ;**
- traitées dans le cadre d'une **médiation, d'une conciliation ou de toute autre procédure alternative de règlement des différends**, en cours ou ayant abouti à la signature d'un protocole d'accord ;
- n'ayant manifestement **aucun caractère sérieux** ;
- portant sur des **éléments imprécis ou invérifiables** ;
- relatives à des **faits trop anciens** empêchant la collecte des éléments de preuve.

Toutefois, lorsque le signalement n'est pas recevable au titre de l'alerte mais porte sur une situation ou une conduite contraire au Code de déontologie et aux procédures internes de CDC Informatique, le déontologue procède à l'instruction du dossier dans le cadre de ses prérogatives.

### ➢ Information des personnes visées et/ou mentionnées dans l'alerte

Conformément à la réglementation applicable[13], **la ou les personne(s) visée(s) par l'alerte, ainsi que les tiers qui y sont mentionnés, sont informé(e)(s) par le déontologue de l'existence de cette alerte**[14],

[12] Il qualifie l'alerte notamment au regard des différentes catégories prévues par la loi (telles que définies au § 1.2.) et s'assure que l'auteur de l'alerte, s'il n'est pas anonyme, appartient à l'une des catégories de bénéficiaires du droit d'alerte mentionnées au § 1.3.
[13] Article 14 du Règlement général sur la protection des données (RGPD)
[14]. Aucune information relative à l'identité de l'émetteur de l'alerte ni, le cas échéant, à celle des tiers n'est communiquée

afin de leur permettre d'exercer leurs droits au titre du traitement de leurs données à caractère personnel (Annexe 1 - Notice d'information sur la protection des données à caractère personnel).

L'information est adressée dans un délai raisonnable, ne pouvant pas dépasser **un mois à compter de la réception de l'alerte**. Toutefois, CDC Informatique se réserve le droit de n'informer la ou les personne(s) faisant l'objet d'une alerte qu'après l'adoption des **mesures conservatoires éventuellement nécessaires, pour notamment prévenir la destruction des preuves relatives à l'alerte**.

Cette information est réalisée selon les modalités permettant de s'assurer de sa bonne délivrance à la personne concernée. Elle ne contient pas d'informations relatives à l'identité de l'émetteur de l'alerte ni à celle de tiers[15].

### ➢ Instruction de l'alerte

Si l'alerte est recevable, le déontologue **vérifie la matérialité des faits,** au besoin en diligentant une enquête interne dans le respect d'une stricte confidentialité telle que précisée au § 3.1.1.

Le déontologue dispose de la compétence, de l'autorité et des moyens suffisants à l'exercice de ses missions. Il réalise ses missions de façon indépendante et impartiale.

A ce titre, le déontologue peut avoir recours, le cas échéant, à des **mesures conservatoires immédiates**, notamment pour prévenir la destruction des preuves relatives à l'alerte.

Il est rappelé que l'altération et la destruction de preuves sont des délits sanctionnés d'une peine de 3 ans d'emprisonnement et de 45.000 euros d'amende (code pénal, art. 434-4).

L'auteur de l'alerte est **informé dans un délai raisonnable n'excédant pas trois mois** à compter de l'accusé de réception[16]du signalement, des mesures envisagées ou prises pour évaluer l'exactitude des allégations et, le cas échéant, remédier à l'objet de l'alerte ainsi que sur les motifs de ces dernières.

Certaines informations relatives au signalement doivent également être partagées avec la personne mise en cause afin de lui donner les moyens de s'expliquer sur les faits concernés. L'information de la personne mise en cause peut être retardée, notamment au titre de l'article 14 paragraphe 5 du RGPD, lorsque le respect de l'obligation d'information est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs du traitement à savoir le traitement de l'enquête liée à l'alerte.

### ➢ Suites données à l'alerte

[15] Référentiel de la CNIL relatif aux traitements de données à caractère personnel destinés à la mise en œuvre d'un dispositif d'alerte en date du 6 juillet 2023.
[16] A défaut d'accusé de réception, le délai de trois mois court à compter de l'expiration d'une période de sept jours ouvrés suivant l'alerte.

A l'issue de l'instruction, sans préjudice des dispositions applicables en matière de confidentialité consacrant notamment la protection accordée au lanceur d'alerte, le déontologue **remet ses conclusions au directeur général**, qui décide, en fonction de la nature des manquements identifiés, d'en informer les directeurs des directions concernées par l'alerte, afin de statuer sur les décisions à prendre, notamment sur la mise en œuvre de sanctions disciplinaires et/ou de mesures idoines (telles que poursuites judiciaires), en coordination notamment avec la DMRCC et la Direction des ressources humaines, ou sur la clôture de l'alerte.

Lorsque l'alerte révèle des défaillances organisationnelles et/ou des manquements sur la mise en œuvre des procédures internes et/ou sur les contrôles internes, des mesures de remédiation individuelles ou collectives sont adoptées par la direction concernée.

➢ **Clôture de l'alerte**

Conformément à l'article 4 du décret n°2022-1284 du 3octobre 2022, l'alerte est clôturée lorsque les allégations sont inexactes ou infondées, ou lorsque l'alerte est devenue sans objet.

L'auteur de l'alerte est alors informé par écrit de la clôture du dossier.

### *2.1.3. Quelles articulations avec les dispositifs spécifiques existants ?*

Ce dispositif a un caractère complémentaire par rapport aux canaux de remontées habituels d'alertes, d'incidents et d'anomalies (par exemple : supérieur hiérarchique, représentants du personnel), notamment lorsque ces derniers s'avèrent inopérants ou inadaptés. L'exercice du droit d'alerte n'est néanmoins pas conditionné à l'usage préalable d'un de ces canaux.

➢ **Cas particulier du signalement d'une situation à risque et/ou de danger physique ou pouvant avoir des conséquences sur la santé mentale, d'une situation de harcèlement, de discrimination, de violence ou d'agissements sexistes au travail**

Outre le recours au dispositif d'alerte interne décrit ci-dessus, ces situations font l'objet, au sein de la CDC Informatique, de dispositifs et d'interlocuteurs spécifiques en lien avec la Direction des ressources humaines. Pour obtenir des informations et connaître les modalités d'alerte mises en place, il convient de se référer aux fiches disponibles sur l'intranet :

https://caissedesdepots.sharepoint.com/sites/ICDC-EspaceRH/SitePages/QUALITE-DE-VIE-AU-TRAVAIL.aspx

**En cas de signalement reçu hors du dispositif interne décrit ci-dessus** et susceptible de constituer une alerte au sens de la présente procédure, la personne et/ou le service qui reçoit l'alerte informe l'auteur du signalement de sa faculté de recourir au dispositif d'alerte interne. Le supérieur hiérarchique qui est destinataire d'une alerte, doit, en outre, transmettre sans délai le signalement ainsi que les

informations qui lui ont été rapportées conformément à ce qui est indiqué au § 2.1.1. « **Qui est destinataire de l'alerte ? »**

### 2.2. Le signalement peut-il être adressé à une autorité externe ?

La personne souhaitant émettre une alerte peut en outre s'adresser à une **instance extérieure** à CDC Informatique, soit après avoir émis cette alerte en interne dans les conditions mentionnées ci-dessus, soit directement :

- à **l'autorité compétente** parmi celles mentionnées en Annexe 2[17] ;
- **au Défenseur des droits**[18], qui l'oriente vers la ou les autorités compétente(s) ;
- **à l'autorité judiciaire**[19] ;
- **à une institution, à un organe ou à un organisme de l'Union européenne** compétent pour recueillir des informations sur des violations du droit de l'Union[20].

Ces instances peuvent être saisies alternativement ou postérieurement à l'usage du dispositif d'alerte interne.

Les autorités externes sont tenues de mettre à disposition, sur leur site internet, les règles de procédure qu'elles appliquent ainsi que les moyens qui permettent de les saisir : courrier, courriel, plateforme *ad hoc* à destination des lanceurs d'alerte. Si la saisine est effectuée par voie postale il est préférable de l'adresser en recommandé selon le système de double enveloppe[21].

Par ailleurs, le lanceur d'alerte peut bénéficier de **mesures d'accompagnement** renforcées telles que précisées en Annexe 3.

### 2.3. Une alerte peut-elle être rendue publique ?

La divulgation publique de l'alerte n'est possible que dans les cas suivants :

- **après avoir effectué un signalement externe, précédé ou non d'un signalement interne, sans qu'aucune mesure appropriée ait été prise en réponse à ce signalement dans le délai de trois mois**[22] ;

[17] L'autorité compétente vers laquelle orienter l'alerte sera à choisir en fonction du domaine concerné par l'alerte
[18] La procédure de communication avec le Défenseur des droits est spécifique ; celle-ci est détaillée sur le site du Défenseur des droits : https://www.defenseurdesdroits.fr .
[19] Le procureur de la République, par exemple : en cas de crime ou délit.
[20] Relevant du champ d'application de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 (par exemple : saisine de L'Office européen de lutte antifraude sur une fraude concernant le budget de l'Union).
[21] Système de double enveloppe : une enveloppe intérieure comprenant les éléments de l'alerte, sur laquelle figure la mention « signalement d'une alerte », la mention « confidentiel » et la date de l'alerte et une enveloppe extérieure à l'adresse de l'autorité
[22] A compter de l'accusé de réception, ou, à défaut d'accusé de réception, trois mois à compter de l'expiration d'une période de 7 jours ouvrés suivant l'alerte. Ce délai peut être porté à six mois si les circonstances particulières de l'affaire, liées notamment à sa nature ou à sa

- **en cas de danger grave et imminent** (pour les alertes qui ne portent pas sur des informations obtenues dans un cadre professionnel) ;

- **en cas de danger imminent ou manifeste pour l'intérêt général**, notamment lorsqu'il existe une situation d'urgence ou un risque de préjudice irréversible, pour les alertes qui portent sur des informations obtenues dans le cadre professionnel[23];

- **lorsque la saisine de l'une des autorités externes ferait encourir à l'auteur de l'alerte un risque de représailles ou qu'elle ne permettrait pas de remédier efficacement à l'objet de la divulgation**, en raison des circonstances particulières de l'affaire[24].

Les trois derniers cas ne s'appliquent pas lorsque la divulgation publique porte atteinte aux intérêts de la défense et de la sécurité nationale.

### 2.4. Où trouver l'information sur le dispositif d'alerte ?

Afin d'assurer à tous les bénéficiaires du droit d'alerte une bonne connaissance du présent dispositif, celui-ci fait l'objet d'une information particulière notamment :

- dans le **Code de déontologie de CDC Informatique**, annexé au règlement intérieur ;

- sur le **site internet de CDC Informatique** (*https://www.icdc.caissedesdepots.fr/)* afin de présenter le dispositif d'alerte interne et les modalités de saisine du déontologue, notamment aux personnes autres que les collaborateurs de CDC Informatique tels que mentionnées au § 1.2. (anciens collaborateurs, candidats à un emploi, collaborateurs extérieurs et occasionnels, prestataires, sous-traitants, etc.) ;

- sur une page dédiée au dispositif d'alerte sur **l'intranet de CDC Informatique** (*https://caissedesdepots.sharepoint.com/sites/WeShare/SitePages/D%C3%89ONTOLOGIE.aspx*) permettant de consulter la présente procédure.

## 3. Protection et droits du lanceur d'alerte

complexité, nécessitent de plus amples diligences. Dans ce cas, l'autorité aura justifié de ces circonstances auprès de l'auteur de l'alerte avant l'expiration du délai de trois mois précédemment mentionnés.

[23] Dans le contexte professionnel, la condition tenant à la gravité du danger n'est pas requise notamment lorsqu'il existe une situation d'urgence ou un risque de préjudice irréversible. Autrement dit, un salarié bénéficie du régime protecteur du lanceur d'alerte s'il divulgue publiquement des informations obtenues dans le cadre de ses activités professionnelles même si la gravité du danger pour l'intérêt général n'est pas caractérisée. Le danger doit cependant être imminent ou manifeste

[24] Notamment si des preuves peuvent être dissimulées ou détruites ou si l'auteur de l'alerte a des motifs sérieux de penser que l'autorité peut être en conflit d'intérêts, en collusion avec l'auteur des faits ou impliquée dans ces faits.

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[25] a consacré un **statut protecteur pour le lanceur d'alerte** dès lors que l'alerte répond à la définition prévue par la loi (rappelée au § 1.) et respecte les modalités de signalement prévues par la présente procédure (précisées au § 2.).

Par ailleurs, la loi n°2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte a étendu certaines protections aux personnes physiques et morales qui sont en lien avec le lanceur d'alerte (*cf*. § 3.2.).

### 3.1. Quelle protection est accordée au lanceur d'alerte ?

#### *3.1.1. Confidentialité*

Conformément à la réglementation (article 9 de la loi du 9 décembre 2016 et à l'article 6 du décret du 3 octobre 2022), la procédure mise en œuvre par CDC Informatique pour recueillir et traiter les alertes internes garantit une **stricte confidentialité de l'identité des auteurs de l'alerte, de la ou des personne(s) visée(s), des tiers mentionnés dans l'alerte**, ainsi que de l'ensemble des informations recueillies par le déontologue.

CDC Informatique prend toutes les mesures et précautions nécessaires pour assurer la sécurité et la confidentialité des données, notamment des données à caractère personnel, tant à l'occasion de leur recueil que de leur traitement et de leur conservation dans le cadre du présent dispositif.

En particulier,

- Le traitement de l'alerte et les échanges avec le lanceur d'alerte et toute personne visée par l'alerte sont effectués au moyen d'une **adresse électronique dont l'accès est restreint** au service Déontologie, tout accès d'une personne non habilitée faisant l'objet d'une détection et d'une vérification de sécurité,
- Tout document et toute information sont **stockés sur un répertoire protégé, dédié et sécurisé** auquel seul le service Déontologie a accès, tout accès d'une personne non habilitée faisant l'objet d'une détection et d'une vérification de sécurité.

Une attention particulière est portée au **respect de la réglementation relative à la protection des données à caractère personnel** dans les différentes phases du dispositif (recueil de l'alerte, instruction de l'alerte, conservation du dossier). Une notice d'information, en Annexe 1 de la présente procédure, précise les modalités du traitement des données à caractère personnel mis en œuvre dans le cadre du présent dispositif d'alerte ainsi que les droits des bénéficiaires du dispositif et des personnes faisant l'objet d'une alerte.

[25] Modifiée par la loi n°2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte.

Durant toute la phase d'instruction, seules les informations pertinentes et nécessaires au regard des finalités du traitement sont collectées et/ou conservées dans le dispositif d'alertes.

Conformément à l'article 9 de la loi du 9 décembre 2016, les éléments d'identification de l'auteur de l'alerte ne peuvent être divulgués qu'avec **son consentement**, sauf en cas de transmission à l'autorité judiciaire, si les personnes chargées du recueil ou du traitement de l'alerte sont tenues de dénoncer les faits à celle-ci. Le lanceur d'alerte en est alors informé, à moins que cette information ne risque de compromettre la procédure judiciaire. Des explications écrites sont jointes à cette information.

Les éléments de nature à identifier la personne mise en cause par un signalement **ne peuvent être divulgués, sauf à l'autorité judiciaire, qu'une fois établi le caractère fondé de l'alerte.**

### *3.1.2. Protection contre toute forme de représailles*

L'auteur de l'alerte est protégé contre toute forme de représailles au cours de la carrière, notamment celles définies :

- à l'article L.1132-3-3 du code du travail qui vise le recrutement, les sanctions disciplinaires, le licenciement ou toute mesure discriminatoire notamment en matière de rémunération, d'intéressement, de formation, de reclassement, d'affectation, de qualification, de promotion professionnelle, de mutation ou de renouvellement de contrat.

Par ailleurs, la loi n°2022-401 du 21 mars 2022 complète la **liste des mesures de représailles interdites** (*cf*. II de l'article 10-1 de la loi n°2016-1691 du 9 décembre 2016 modifiée) :

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° Evaluation 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 à durée déterminée ou d'un contrat 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 à durée déterminée ou d'un contrat temporaire ;

11° 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 ;

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 dans le secteur ou 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 abusive vers un traitement psychiatrique ou médical.

Dans les mêmes conditions, les autres bénéficiaires du droit d'alerte tels que définis au § 1.2. ne peuvent faire l'objet de mesures de représailles, ni de menaces ou de tentatives de recourir à ces mesures.

Toute mesure de représailles, menaces ou tentatives de recourir à ces mesures, à l'encontre d'une personne qui a signalé une alerte est nulle de plein droit, ne saurait être tolérée et donnera lieu à des sanctions disciplinaires pouvant aller jusqu'à la rupture du contrat de travail, conformément au droit applicable.

### *3.1.3. Irresponsabilités pénale et civile*

Conformément à l'article 122-9 du code pénal, **lorsque son signalement porte atteinte à un secret protégé par la loi,** le lanceur d'alerte bénéficie d'une **irresponsabilité pénale**[26] dès lors que cette divulgation est nécessaire et proportionnée à la sauvegarde des intérêts en cause, qu'elle intervient dans le respect des conditions de signalement définies par la loi.

Le lanceur d'alerte n'est pas non plus pénalement responsable s'il soustrait, détourne ou recèle des documents ou tout autre support contenant les informations qu'il signale ou divulgue, à condition qu'il en ait eu connaissance de manière licite[27].

[26] Sont exclus de cette irresponsabilité pénale les faits, informations et documents couverts par le secret de la défense nationale, le secret médical, le secret des délibérations judiciaires, le secret de l'enquête ou de l'instruction judiciaires ou le secret professionnel de l'avocat

[27] Et non, par exemple, dans le cadre d'une intrusion irrégulière dans un lieu ou d'un vol.

Par ailleurs, le lanceur d'alerte bénéficie également d'une **irresponsabilité civile pour les dommages causés du fait de ce signalement** dès lors qu'il avait des motifs raisonnables de croire, au moment du signalement ou de la divulgation publique, que l'alerte était nécessaire à la sauvegarde des intérêts en cause.

### 3.2. Est-il prévu une protection pour l'entourage du lanceur d'alerte ?

La loi n° 2022-401 du 21 mars 2022 (article 6.1) a étendu les protections à un certain nombre d'acteurs ayant un lien avec le lanceur d'alerte. Il s'agit des :

- **facilitateurs**, entendus au sens de ladite loi comme toute personne physique ou morale de droit privé à but non lucratif (syndicats, associations) qui aide le lanceur d'alerte à effectuer son signalement ou une divulgation ;

- **personnes physiques en lien avec le lanceur d'alerte** (collègues, proches) et risquant de faire l'objet d'une mesure de représailles dans le cadre de leurs activités professionnelles de la part de leur employeur, de leur client ou du destinataire de leurs services ;

- **entités juridiques contrôlées** (société civile ou commerciale, association dotée ou non de la personnalité juridique) **par le lanceur d'alerte**, pour lesquelles il travaille ou avec lesquelles il est en lien dans un contexte professionnel.

## 4. Les sanctions encourues en cas d'alerte effectuée dans l'intention de nuire

De même, l'utilisation de mauvaise foi du dispositif d'alerte, notamment lorsque les alertes sont effectuées dans l'intention de nuire à la réputation d'une ou plusieurs personnes physiques ou morales, ou dans le cas d'alertes intentionnellement mensongères, expose leurs auteurs à des sanctions disciplinaires ainsi qu'à des poursuites judiciaires sur le fondement du délit de dénonciation calomnieuse.

En application de l'article 226-10 du code pénal, la dénonciation calomnieuse d'un fait de nature à entraîner des sanctions judiciaires, administratives ou disciplinaires, définie comme celle effectuée de mauvaise foi par une personne consciente du caractère infondé de cette dénonciation, est sanctionnée d'un emprisonnement pouvant atteindre cinq ans et d'une amende de 45.000 euros, ces deux peines pouvant être cumulatives ou alternatives. L'auteur d'une dénonciation calomnieuse peut également être condamné à verser à la victime des dommages et intérêts en réparation des préjudices subis.

Par ailleurs, afin de préserver les vertus de la démarche d'alerte, et d'empêcher qu'elle soit utilisée à mauvais escient et à l'encontre des intérêts de protection des droits des personnes impliquées, des sanctions pouvant aller jusqu'à la rupture de la relation contractuelle, ou encore des poursuites judiciaires pourront être engagées, en cas de :

- obstacle ou tentative d'entrave, par son action ou inaction, à un signalement ou au traitement d'un signalement ;
- violation de l'obligation de confidentialité liée au recueil d'un signalement ou à son traitement ;
- exercice de représailles ou menaces de représailles, ou toute forme de procédures abusives à l'encontre de l'auteur d'un signalement, des facilitateurs ou tiers en lien avec l'auteur du signalement.

## Annexe n°1 : Notice d'information sur la protection des données à caractère personnel

Nous vous informons que vos données à caractère personnel recueillies dans le cadre du dispositif d'alerte sont susceptibles de faire l'objet d'un traitement par CDC Informatique dont le siège est situé 18 avenue Aristide Briand, 92220 Bagneux.

Les données collectées sont destinées à être utilisées le déontologue, les autres personnes composant le service Déontologie, et, le cas échéant, la Direction des ressources humaines, le Déontologue de la Caisse des Dépôts l'Inspecteur général, directeur de l'audit du Groupe, des prestataires externes et/ou cabinets d'avocats, autres contributeurs temporaires pour le traitement des alertes.

A noter que tous les prestataires externes ou autres contributeurs temporaires susceptibles d'intervenir dans le cadre du traitement d'une alerte sont soumis à une obligation de confidentialité renforcée par la signature d'un engagement de confidentialité leur rappelant leurs obligations et les sanctions associées

Vos données seront utilisées pour le signalement et le traitement des alertes émises par une personne physique en application de la réglementation, en particulier 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, modifiée par la loi n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte et précisée par le décret n°2022-1284 du 3 octobre 2022, ainsi que du Code de déontologie de CDC Informatique.

Ainsi, le traitement des données personnelles est mis en œuvre afin de :

- recueillir et traiter les alertes entrant dans le champ d'application de l' article 6 de la loi du 9 décembre 2016 susvisée ;
- effectuer les vérification, enquêtes et analyses nécessaires ;
- définir les suites à donner au signalement ;
- assurer la protection des personnes concernées ;
- exercer ou défendre des droits en justice ;
- effectuer des statistiques sur la base des données anonymisées[28].

Les catégories de données traitées sont :

- alerte (les faits signalés) ;

[28] Référentiel de la CNIL en date du 6 juillet 2023 relatif aux traitements de données à caractère personnel destinées à la mise en œuvre d'un dispositif d'alerte

- identité, fonction, coordonnées de l'émetteur de l'alerte, des personnes faisant l'objet de l'alerte, des personnes intervenants, consultées ou entendues dans le recueil ou dans le traitement de l'alerte, des facilitateurs, et personnes en lien avec l'émetteur de l'alerte ;
- les éléments recueillies dans le cadre de la vérification des faits signalés ;
- compte rendu des opérations de vérification ;
- suite donnée à l'alerte [29];
- statistiques d'activités .

Par ailleurs, afin d'assurer le respect du principe de minimisation des données, il est expressément demandé au lanceur d'alerte de limiter les informations communiquées aux seuls faits nécessaires à la description de l'alerte. Il est notamment invité à ne pas inclure d'informations révélant des données sensibles au sens de l'article 9 (1) RGPD, notamment la vie privée de tiers, la santé de tiers, l'appartenance syndicale de tiers, sauf si ces éléments sont strictement indispensables à la compréhension du signalement. Toute communication de données sensibles non pertinentes est supprimée ou anonymisée.

La base légale du traitement est ventilée comme suit :

| SOUS-FINALITE | BASE LEGALE |
|---|---|
| • recueillir et traiter les alertes entrant dans le champ d'application de l' article 6 de la loi du 9 décembre 2016 | Respect d'une obligation légale à laquelle le responsable du traitement est soumis |
| • effectuer les vérification, enquêtes et analyses nécessaires | |
| • définir les suites à donner au signalement | |
| • assurer la protection des personnes concernées | |
| • exercer ou défendre des droits en justice | |
| • effectuer des statistiques d'activités | Intérêt légitime poursuivi par le responsable du traitement ou par un tiers |

[29] Référentiel de la CNIL en date du 6 juillet 2023 relatif aux traitements de données à caractère personnel destinées à la mise en œuvre d'un dispositif d'alerte

Dans le cadre du présent traitement, des données sensibles peuvent être traitées sur le fondement de l'article 9 (2) g) et 9 (2) f) du RGPD[30].

Vos données sont susceptibles d'être conservées pendant une durée maximale de :

- 12 mois après la clôture des vérifications lorsqu'un signalement n'a fait l'objet d'aucune suite ;
- 5 ans après la clôture de l'alerte en cas de suites données à l'alerte ;
- jusqu'au terme de la procédure disciplinaire engagée à l'encontre de la personne mise en cause ou de l'auteur d'un signalement abusif ;
- jusqu'à la fin du litige, en ce compris l'épuisement de toute voie de recours possible lorsque des poursuites judiciaires sont engagées à l'encontre de la personne mise en cause ou de l'auteur d'un signalement abusif.

Dans le cas où l'alerte est considérée comme irrecevable, tout élément du dossier de signalement de nature à permettre l'identification de l'auteur du signalement est détruit dans un délai qui ne peut excéder 2 mois à compter la clôture des opérations de vérification de la recevabilité de l'alerte.

Les données relatives au signalement sont détruites ou anonymisées à l'issue de leur durée de conservation.

Vous disposez, en tant que bénéficiaire du dispositif d'alerte et/ou en tant que personne faisant l'objet d'un signalement, d'un droit d'accès aux données, de rectification des données vous concernant, ainsi que du droit d'en faire limiter l'usage.

Il est précisé que la personne qui fait l'objet d'un signalement ne peut en aucun cas obtenir communication du déontologue, des informations concernant l'identité du lanceur d'alerte au titre du droit d'accès prévu par l'article 15 du RGPD.

Par ailleurs, le droit de rectification ne doit pas permettre la modification rétroactive des éléments contenus dans l'alerte ou collectées lors de son instruction. Son exercice ne doit pas aboutir à l'impossibilité de reconstitution de la chronologie des éventuelles modifications d'éléments importants de l'enquête. Aussi, ce droit ne peut-il être exercé que pour rectifier les données factuelles, dont l'exactitude matérielle peut être vérifiée par le déontologue à l'appui d'éléments probants, et ce, sans que soient effacées ou remplacées les données, même erronées, collectées initialement[31].

Pour exercer vos droits, vous pouvez :

[30] Référentiel de la CNIL en date du 6 juillet 2023 relatif aux traitements de données à caractère personnel destinées à la mise en œuvre d'un dispositif d'alerte.
[31] Référentiel de la CNIL en date du 6 juillet 2023 relatif aux traitements de données à caractère personnel destinées à la mise en œuvre d'un dispositif d'alerte.

- écrire à l'adresse suivante : CDC Informatique – à l'attention du Délégué à la protection des données personnelles (DPO) – 18 avenue Aristide Briand, 92220 Bagneux ; ou

- adresser un courriel à DPO-ICDC@caissedesdepots.fr,

et y joindre, le cas échéant, toute pièce permettant de justifier votre identité et votre demande.

Si vous considérez que CDC Informatique n'a pas respecté vos droits, vous disposez du droit d'introduire une réclamation auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL), autorité de contrôle chargé du respect des obligations en matière de données à caractère personnel.

Pour toute information complémentaire ou question relative à vos droits ou à l'utilisation de vos données, vous pouvez contacter le délégué à la protection des données (DPO) à l'adresse suivante : à DPO-ICDC@caissedesdepots.fr.

| | | |
|---|---|---|
| CDC INFORMATIQUE | Date d'application 15/05/2026<br><br>Accès public | **Sous-domaine : Politique et stratégie de l'entreprise**<br>**Procédure relative au dispositif d'alerte professionnelle de CDC Informatique** |
| **Domaine : Pilotage** | Responsable de la procédure :<br>Direction de la Maitrise des Risques, du Contrôle permanent, de la Conformité et de la Déontologie de CDC Informatique (DMRCC ICDC) | **V1** |

## Annexe n°2 : Liste des autorités externes[32]

Le lanceur d'alerte choisit l'autorité dont le champ de compétence correspond le mieux à l'objet de l'alerte[33].

**1. Marchés publics :**

- Agence française anticorruption (AFA), pour les atteintes à la probité ;

- Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF), pour les pratiques anticoncurrentielles ;

- Autorité de la concurrence, pour les pratiques anticoncurrentielles ;

**2. Services, produits et marchés financiers et prévention du blanchiment de capitaux et du financement du terrorisme :**

- Autorité des marchés financiers (AMF), pour les prestataires en services d'investissement et infrastructures de marchés ;

- Autorité de contrôle prudentiel et de résolution (ACPR), pour les établissements de crédit et organismes d'assurance ;

**3. Sécurité et conformité des produits :**

- Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) ;

- Service central des armes et explosifs (SCAE) ;

**4. Sécurité des transports :**

- Direction générale de l'aviation civile (DGAC), pour la sécurité des transports aériens ;

- Bureau d'enquêtes sur les accidents de transport terrestre (BEA-TT), pour la sécurité des transports terrestres (route et fer) ;

- Direction générale des affaires maritimes, de la pêche et de l'aquaculture (DGAMPA), pour la sécurité des transports maritimes ;

[32] Prévue à l'annexe du Décret n° 2022-1284 du 3 octobre 2022

[33] Par exemple : pour une alerte concernant les activités du ministère de la Défense, le contrôle général des armées ; pour une alerte portant sur des faits de corruption, l'Agence française anticorruption

**5. Protection de l'environnement :**

- Inspection générale de l'environnement et du développement durable (IGEDD) ;

**6. Radioprotection et sûreté nucléaire :**

- Autorité de sûreté nucléaire (ASN) ;

**7. Sécurité des aliments :**

- Conseil général de l'alimentation, de l'agriculture et des espaces ruraux (CGAAER) ;

- Agence nationale chargée de la sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES) ;

**8. Santé publique :**

- Agence nationale chargée de la sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES) ;

- Agence nationale de santé publique (Santé publique France, SpF) ;

- Haute Autorité de santé (HAS) ;

- Agence de la biomédecine ;

- Etablissement français du sang (EFS) ;

- Comité d'indemnisation des victimes des essais nucléaires (CIVEN) ;

- Inspection générale des affaires sociales (IGAS) ;

- Institut national de la santé et de la recherche médicale (INSERM) ;

- Conseil national de l'ordre des médecins, pour l'exercice de la profession de médecin ;

- Conseil national de l'ordre des masseurs-kinésithérapeutes, pour l'exercice de la profession de masseur-kinésithérapeute ;

- Conseil national de l'ordre des sages-femmes, pour l'exercice de la profession de sage-femme ;

- Conseil national de l'ordre des pharmaciens, pour l'exercice de la profession de pharmacien ;

- Conseil national de l'ordre des infirmiers, pour l'exercice de la profession d'infirmier ;

- Conseil national de l'ordre des chirurgiens-dentistes, pour l'exercice de la profession de chirurgien-dentiste ;

- Conseil national de l'ordre des pédicures-podologues, pour l'exercice de la profession de pédicure-podologue ;

- Conseil national de l'ordre des vétérinaires, pour l'exercice de la profession de vétérinaire ;

**9. Protection des consommateurs :**

- Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) ;

**10. Protection de la vie privée et des données personnelles, sécurité des réseaux et des systèmes d'information :**

- Commission nationale de l'informatique et des libertés (CNIL) ;

- Agence nationale de la sécurité des systèmes d'information (ANSSI) ;

**11. Violations portant atteinte aux intérêts financiers de l'Union européenne :**

- Agence française anticorruption (AFA), pour les atteintes à la probité ;

- Direction générale des finances publiques (DGFIP), pour la fraude à la taxe sur la valeur ajoutée ;

- Direction générale des douanes et droits indirects (DGDDI), pour la fraude aux droits de douane, droits anti-dumping et assimilés ;

**12. Violations relatives au marché intérieur :**

- Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF), pour les pratiques anticoncurrentielles ;

- Autorité de la concurrence, pour les pratiques anticoncurrentielles et les aides d'Etat ;

- Direction générale des finances publiques (DGFIP), pour la fraude à l'impôt sur les sociétés ;

**13. Activités conduites par le ministère de la défense :**

- Contrôle général des armées (CGA) ;

- Collège des inspecteurs généraux des armées ;

**14. Statistique publique :**

- Autorité de la statistique publique (ASP) ;

**15. Agriculture :**

- Conseil général de l'alimentation, de l'agriculture et des espaces ruraux (CGAAER) ;

**16. Education nationale et enseignement supérieur :**

- Médiateur de l'éducation nationale et de l'enseignement supérieur ;

**17. Relations individuelles et collectives du travail, conditions de travail :**

- Direction générale du travail (DGT) ;

**18. Emploi et formation professionnelle :**

- Délégation générale à l'emploi et à la formation professionnelle (DGEFP) ;

**19. Culture :**

- Conseil national de l'ordre des architectes, pour l'exercice de la profession d'architecte ;

- Conseil des maisons de vente, pour les enchères publiques ;

**20. Droits et libertés dans le cadre des relations avec les administrations de l'Etat, les collectivités territoriales, les établissements publics et les organismes investis d'une mission de service public :**

- Défenseur des droits ;

**21. Intérêt supérieur et droits de l'enfant :**

- Défenseur des droits ;

**22. Discriminations :**

- Défenseur des droits ;

**23. Déontologie des personnes exerçant des activités de sécurité :**

- Défenseur des droits.

## Annexe n°3 : Mesures d'accompagnement du lanceur d'alerte

La loi n°2022-401 du 21 mars 2022 renforce l'accompagnement du lanceur d'alerte dont les principales mesures sont rappelées ci-après.

***Appui du Défenseur des droits***

Le Défenseur des droits, outre son rôle d'orientation, doit informer et conseiller le lanceur d'alerte et défendre ses droits et libertés. Cette protection est étendue aux autres personnes protégées dans le cadre d'une procédure d'alerte, en particulier les tiers et les « facilitateurs » (cf. 3.2 de la procédure). Ces missions sont assurées par l'adjoint au Défenseur des droits chargé de l'accompagnement des lanceurs d'alerte.

Par ailleurs, toute personne peut demander au Défenseur des droits de certifier sa qualité de lanceur d'alerte. Cette certification prend la forme d'un avis[34]. Cette reconnaissance formelle permet de faciliter l'accès du lanceur d'alerte aux diverses mesures de protection contre les représailles et les procédures bâillons ainsi qu'un accès privilégié aux dispositifs de soutien financier visant à améliorer la protection des lanceurs d'alerte (cf. infra).

***Soutien financier en cours de procédure judiciaire***

Pour limiter le coût financier des procédures engagées par le lanceur d'alerte (pour contester une mesure de représailles) ou contre lui (procédure "bâillon" comme une plainte pour diffamation destinée à l'intimider et le réduire au silence), le juge peut accorder, en début d'instance, une provision pour frais de justice supportée par la partie adverse, au lanceur d'alerte qui justifie avoir procédé

[34] Une réponse doit être apportée à l'intéressé dans un délai de six mois.

conformément à la loi et que la mesure qu'il conteste, ou la procédure engagée contre lui, constitue une représailles ou vise à entraver son alerte. Dans les mêmes conditions, le juge a également la possibilité d'allouer une provision, pour couvrir ses subsides, au lanceur d'alerte dont la situation financière s'est gravement dégradée en raison de l'alerte. Ces provisions peuvent être rendues définitives par le juge à tout moment, c'est-à-dire même si le lanceur d'alerte perd son procès.

***Soutien psychologique et financier par les autorités externes***

Le lanceur d'alerte peut bénéficier de mesures de soutien psychologique et financier par les autorités externes, qu'elles aient été saisies directement ou via le Défenseur des droits. Il s'agit d'une simple faculté pour ces autorités et non d'une obligation. La loi renvoie à chaque autorité compétente le soin de décider du principe et des conditions d'un tel soutien.

## Annexe n°4 : Modèle de formulaire de signalement