ethicorp.com

## DISPOSITIF D'ALERTES PROFESSIONNELLES

# PROCEDURE DE RECUEIL DES SIGNALEMENTS

### INTRODUCTION

L'entreprise a souscrit au dispositif d'alertes, **ethicorp.com**.

Ce dispositif s'inscrit dans la démarche éthique de l'entreprise, qui vise à établir et pérenniser une culture d'intégrité, de transparence et d'intégrité.

La présente procédure vise à rappeler le cadre légal des dispositifs d'alertes, les droits, garanties et devoirs des salariés et collaborateurs externes et occasionnels, les principes et modalités de fonctionnement du dispositif.

Elle est complétée par le mode d'emploi précis du dispositif ainsi que par des formations dédiées.

### Article 1. CADRE LÉGAL DE LA MISE EN PLACE DU DISPOSITIF D'ALERTES PROFESSIONNELLES

La **loi n°2016-1691 du 9 décembre 2016**[1] relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, dite Loi Sapin II, a été révisée par la **loi n° 2022-401 du 21 mars 2022** visant à améliorer la protection des lanceurs d'alerte, ayant donné lieu au **décret n°2022-1284 du 3 octobre 2022** relatif aux procédures de recueil et de traitement des signalements émis par les lanceurs d'alerte.

La loi Sapin II révisée comporte **deux dispositions** complémentaires imposant la mise en place de dispositifs de signalement, révisées par la loi n° :

- Article 8, I. B : « ***Sont tenues d'établir une procédure interne de recueil et de traitement des signalements****, après consultation des instances de dialogue social et dans les conditions fixées par décret en Conseil d'État :*
  *1° Les personnes morales de droit public employant au moins cinquante agents, à l'exclusion des communes de moins de 10 000 habitants, des établissements publics qui leur sont rattachés et des établissements publics de coopération intercommunale qui ne comprennent parmi leurs membres aucune commune excédant ce seuil de population ;*
  *2° Les administrations de l'État ;*
  *3° Les personnes morales de droit privé et les entreprises exploitées en leur nom propre par une ou plusieurs personnes physiques, employant au moins cinquante salariés ;*
  *4° Toute autre entité relevant du champ d'application des actes de l'Union européenne mentionnés au B de la partie I et à la partie II de l'annexe à 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.* »

[1] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033558528

ethicorp.com

- Article 17, II : *« Les personnes mentionnées au I*[2] *mettent en œuvre (…) un* ***dispositif d'alerte interne destiné à permettre le recueil des signalements*** *émanant d'employés et relatifs à l'existence de conduites ou de situations contraires au code de conduite de la société »*.

Conformément aux Recommandations de l'Agence française anticorruption[3], il est possible de mettre en place un seul et unique dispositif technique de recueil des signalements commun aux deux dispositions.

La mise en œuvre des dispositifs d'alertes est par ailleurs encadrée par :

- Le **Règlement Général sur la Protection des Données (RGPD)** du Parlement européen du 14 avril 2016 ;
- La loi n° 78-17 du 6 janvier 1978 relative à **l'informatique, aux fichiers et aux libertés** (révisée conformément aux dispositions du RGPD) ;
- Les **Recommandations de l'Agence française anticorruption** (AFA)[4].

**Important : Toute personne qui fait obstacle, de quelque façon que ce soit, à la transmission d'une alerte est punie d'un an d'emprisonnement et 15 000 euros d'amende (75 000 euros pour les personnes morales).**

## Article 2. DÉFINITION DU LANCEUR D'ALERTE – OUVERTURE DU DISPOSITIF

L'article 6 de la Loi Sapin II révisée définit le lanceur d'alerte :

> *« Un 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. Lorsque les informations n'ont pas été obtenues dans le cadre des activités professionnelles mentionnées au I de l'article 8, le lanceur d'alerte doit en avoir eu personnellement connaissance. »*

Ainsi, le lanceur d'alerte doit être :

- Une **personne physique** – ce ne peut pas être une personne morale, c'est-à-dire une entreprise, une association ou même un syndicat ;
- **Sans contrepartie financière directe** – en France le lanceur d'alerte n'est pas rémunéré ;
- **De bonne foi** – le lanceur d'alerte ne doit pas agir de façon malveillante ou par vengeance en colportant des informations qu'il sait mensongères ou erronées ;
- Lorsque les informations n'ont pas été obtenues dans le cadre des activités professionnelles, le lanceur d'alerte doit en avoir eu personnellement connaissance, c'est-à-dire en avoir été le **témoin personnel** des faits (ou la victime) – le lanceur d'alerte ne peut pas colporter une simple rumeur.

---

[2] Article 17, I : *« les présidents, les directeurs généraux et les gérants d'une société employant au moins cinq cents salariés, ou appartenant à un groupe de sociétés dont la société mère a son siège social en France et dont l'effectif comprend au moins cinq cents salariés, et dont le chiffre d'affaires ou le chiffre d'affaires consolidé est supérieur à 100 millions d'euros »*

[3] https://www.economie.gouv.fr/files/files/directions_services/afa/2017_-_Recommandations_AFA.pdf

[4] Voir supra

ethicorp.com

C'est à ces conditions que le lanceur d'alerte bénéficiera des pleines protections garanties par la loi (voir infra l'article « **Les protections du lanceur d'alerte** ». À défaut, en cas notamment de mauvaise foi, de colportage de rumeurs ou de faits diffamatoires, il ou elle s'exposera à des sanctions.

La faculté de déposer une alerte est légalement ouverte :

- Aux membres du personnel,
- Aux personnes dont la relation de travail s'est terminée, lorsque les informations ont été obtenues dans le cadre de cette relation,
- Aux personnes qui se sont portées candidates à un emploi au sein de l'entité concernée, lorsque les informations ont été obtenues dans le cadre de cette candidature ;
- Aux actionnaires, aux associés et aux titulaires de droits de vote au sein de l'assemblée générale de l'entité ;
- Aux membres de l'organe d'administration, de direction ou de surveillance ;
- Aux collaborateurs extérieurs et occasionnels ;
- Aux cocontractants de l'entité concernée, à leurs sous-traitants ou, lorsqu'il s'agit de personnes morales, aux membres de l'organe d'administration, de direction ou de surveillance de ces cocontractants et sous-traitants,
- Ainsi qu'aux membres du personnel des cocontractants et sous-traitants.

### Article 3. À QUI TRANSMETTRE L'ALERTE ?

Le lanceur d'alerte dispose de **trois canaux distincts** pour effectuer son signalement tout en bénéficiant des protections accordées par la loi à ce statut :

- **Signalement interne** : le lanceur d'alerte choisit de déposer l'alerte en interne auprès de sa hiérarchie ou via la plateforme ethicorp.com,
- **Signalement externe** : le lanceur d'alerte peut adresser son alerte à une autorité compétente (listée par décret), au Défenseur des droits, à l'autorité judiciaire ou à toute institution, organe ou organisme de l'Union européenne compétent, soit après un signalement interne soit directement, lorsqu'il estime qu'il n'est pas possible de remédier efficacement à la violation par un signalement interne ou qu'il ne s'expose à un risque de représailles
- **Divulgation publique** : Le lanceur d'alertes peut enfin rendre l'alerte publique, soit pour le lanceur d'alerte qui a obtenu les informations dans le cadre de ses activités professionnelles en cas de danger imminent ou manifeste pour l'intérêt général, soit si le signalement externe n'a été suivi d'aucune mesure appropriée dans les délais fixés, en cas de danger grave et imminent ou lorsque la saisine de l'autorité compétente ferait courir au lanceur d'alerte un risque de représailles ou ne permettrait pas de remédier efficacement à la situation.

**Pour apporter les plus hautes garanties d'impartialité et d'indépendance, l'entreprise a choisi comme référent ethicorp.com, accessible à l'adresse https://www.ethicorp.com.**

Cette plateforme de réception et traitement des alertes est entièrement gérée et administrée par des **avocats**, professionnels réglementés indépendants, astreints à des obligations déontologiques et disciplinaires strictes, notamment en matière de confidentialité et secret professionnel.

**ethicorp.com** dispose ainsi, par son positionnement, de la compétence, de l'autorité et des moyens suffisants à l'exercice de ses missions.

ethicorp.com

### Article 4. QUE DÉCLARER : LES FAITS OBJETS DE L'ALERTE

Conformément à la loi, une alerte peut porter sur :

- Un **crime ou 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 ;**
    - **Ou d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement ;**
    - **Ou du droit de l'Union européenne, de la loi ou du règlement.**
- Un **manquement au Code de conduite anti-corruption** (en cas d'applicabilité de l'article 17 de la loi).

**L'alerte peut porter sur des faits qui se sont produits ou qui sont très susceptibles de se produire.**

**Quelques exemples :**

- Abus de bien social
- Atteintes aux règles d'hygiène
- Blanchiment
- Concurrence déloyale
- Conflits d'intérêts
- Corruption privée
- Corruption publique
- Délit d'entrave
- Détournements de fonds
- Discrimination
- Escroquerie
- Favoritisme
- Fraude au président / fournisseur
- Fraude fiscale
- Harcèlement moral
- Harcèlement sexuel
- Intrusion informatique
- Protection des données personnelles
- Radicalisation et terrorisme
- Réglementation sectorielle (assurances, mutuelles, sécurité sociale)
- Risque industriel
- Sécurité des salariés et accidents du travail
- Violation de confidentialité - secret
- Violences - agressions
- Vols
- etc.

En cas de doute, il est préférable d'utiliser le dispositif plutôt que de prendre le risque qu'un fait grave mal sous-estimé ne soit pas révélé. Les avocats intervenant via **ethicorp.com** ont la compétence nécessaire pour examiner l'alerte et apprécier de son opportunité.

### Article 5. CONFIDENTIALITÉ

Conformément à l'article 9 de la loi du 9 décembre 2016, *« Les procédures mises en œuvre pour recueillir et traiter les signalements, dans les conditions mentionnées à l'article 8, garantissent une stricte confidentialité de* ***l'identité des auteurs du signalement, des personnes visées par celui-ci et de tout tiers mentionné dans le signalement et des informations recueillies par l'ensemble des destinataires du signalement****. »*

Doivent donc demeurer strictement confidentiels :

- **L'identité du lanceur d'alerte**, qui doit pouvoir ainsi déposer son alerte en toute tranquillité ;
- **L'identité de la personne visée** par l'alerte et de **tout tiers mentionné** dans le signalement ;
- **Les informations recueillies** dans le cadre de l'alerte, c'est à dire les faits objets de l'alerte.

Ces deux derniers éléments (identité de la personne visée et de tout tiers mentionné dans le signalement et informations recueillies dans le cadre de l'alerte) ne seront en pratique transmises qu'au Comité d'éthique et aux personnes chargées d'enquêter sur les faits.

ethicorp.com

La CNIL précise dans sa délibération du 18 juillet 2019 concernant notamment les responsables du traitement externe que « *Le référent ou prestataire de service* […] *s'engage notamment, par voie contractuelle, à ne pas utiliser les données à des fins autres que la gestion des alertes,* ***à assurer leur confidentialité*** *[…]* »

Par ailleurs, le lanceur d'alerte ne peut pas lui-même divulguer librement les informations objet de l'alerte.

**Important** – Toute violation de la confidentialité de l'alerte est punie de **deux ans d'emprisonnement**, et **30 000 euros d'amende** (**150 000 euros** pour les personnes morales)[5].

**Anonymat éventuel du lanceur d'alerte**

La CNIL (délibération du 18 juillet 2019) recommande que l'organisme n'incite pas les personnes ayant vocation à utiliser le dispositif à le faire de manière anonyme. Son identité est cependant traitée de manière **confidentielle**.

Par exception au principe de s'identifier, la CNIL précise que l'alerte d'une personne qui souhaite rester **anonyme** peut être traitée sous deux conditions cumulatives :

- **La gravité des faits mentionnés est établie et les faits suffisamment détaillés**, il sera donc indispensable d'être précis dans le descriptif des faits ;
- Le traitement de l'alerte s'entoure de **précautions particulières**, notamment un examen préalable par son premier destinataire de l'opportunité de sa diffusion, ce qui est par principe le cas avec les avocats intervenant via la plateforme **ethicorp.com**.

Si ces conditions ne sont pas réunies, les avocats intervenant via **ethicorp.com** pourront informer le lanceur d'alerte qu'il ou elle doit s'identifier (auprès d'ethicorp.com exclusivement et sous garantie de confidentialité) ou qu'à défaut l'alerte ne pourra pas être traitée.

En pratique, si le lanceur d'alerte fournit son identité, seule **ethicorp.com** en sera informée, **l'identité ne sera pas transmise ou révélée à l'employeur**. **ethicorp.com** ne transmettra, dans les conditions strictes de la loi rappelées *supra*, que les faits objets de l'alerte et l'identité de la personne visée, de manière à permettre l'enquête interne sur les faits. L'entreprise s'est par ailleurs engagée contractuellement avec **ethicorp.com** à ne pas demander ni tenter de rechercher l'identité du lanceur d'alerte.

Enfin, pour éviter toute inquiétude, il est recommandé de ne pas utiliser le matériel de l'entreprise pour se connecter à la plateforme **ethicorp.com** ni d'utiliser son adresse électronique professionnelle pour créer son compte de lanceur d'alerte.

## Article 6. LES PROTECTIONS ET DEVOIRS DU LANCEUR D'ALERTE

Conformément à l'article 10-1 et 12 à 13-1 de la loi Sapin II révisée, le lanceur d'alerte bénéficie d'une **protection contre toute mesure de rétorsion**.

Article L. 1121-2 du Code du travail :

> *« Aucune personne ne peut être écartée d'une procédure de recrutement ou de l'accès à un stage ou à une période de formation professionnelle, aucun salarié ne peut être sanctionné, licencié ou faire l'objet d'une mesure discriminatoire, directe ou indirecte, notamment en matière de rémunération, au sens de l'article L. 3221-3, de mesures d'intéressement ou de distribution d'actions, de formation,*

[5] Article 9, II de la loi du 9 décembre 2016

ethicorp.com

*de reclassement, d'affectation, de qualification, de classification, de promotion professionnelle, d'horaires de travail, d'évaluation de la performance, de mutation ou de renouvellement de contrat, ni de toute autre mesure mentionnée au II de l'article 10-1 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, pour avoir signalé ou divulgué des informations dans les conditions prévues aux articles 6 et 8 de la même loi. »*

Article L. 1132-3-3 du Code du travail :

*« Aucune personne ayant témoigné, de bonne foi, de faits constitutifs d'un délit ou d'un crime dont elle a eu connaissance dans l'exercice de ses fonctions ou ayant relaté de tels faits ne peut faire l'objet des mesures mentionnées à l'article L. 1121-2.*

*Les personnes mentionnées au premier alinéa du présent article bénéficient des protections prévues aux I et III de l'article 10-1 et aux articles 12 à 13-1 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. »*

Art. L. 1152-2 du Code du travail

*« Aucune personne ayant subi ou refusé de subir des agissements répétés de harcèlement moral ou ayant, de bonne foi, relaté ou témoigné de tels agissements ne peut faire l'objet des mesures mentionnées à l'article L. 1121-2.*

Les mesures de rétorsion contre un lanceur d'alerte constituent par ailleurs un délit de discrimination, conformément à l'article 225-1 du Code pénal.

Le lanceur d'alerte bénéficie également, dans certains cas à certaines conditions, d'une **irresponsabilité pénale et civile**.

En effet, conformément à l'article 122-9 du Code pénal :

*« N'est pas pénalement responsable **la personne qui porte atteinte à un secret protégé par la loi**, dès lors que cette divulgation est **nécessaire et proportionnée à la sauvegarde des intérêts en cause, qu'elle intervient dans le respect des conditions de signalement définies par la loi et que la personne répond aux critères de définition du lanceur d'alerte** prévus à l'article 6 de la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.*

*N'est pas non plus pénalement responsable le lanceur d'alerte qui **soustrait, détourne ou recèle les documents ou tout autre support contenant les informations dont il a eu connaissance de manière licite** et qu'il signale ou divulgue dans les conditions mentionnées au premier alinéa du présent article.*

*Le présent article est également applicable au complice de ces infractions. »*

Par exception, l'alerte ne peut pas porter sur des éléments couverts par le secret de la défense nationale, le secret médical ou le secret des relations entre un avocat et son client.

Par ailleurs, l'article 10-1 de la Loi Sapin II prévoit, depuis l'entrée en vigueur de la loi n°2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte[6], une irresponsabilité civile des lanceurs d'alerte ayant choisi la voie de la divulgation publique, à certaines conditions :

*« Les personnes ayant signalé ou divulgué publiquement des informations dans les conditions prévues aux articles 6 et 8 ne sont pas civilement responsables des dommages causés du fait de*

[6] LOI n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte (1) - Légifrance (legifrance.gouv.fr)

ethicorp.com

*leur signalement ou de leur divulgation publique* ***dès lors qu'elles avaient des motifs raisonnables de croire, lorsqu'elles y ont procédé, que le signalement ou la divulgation publique de l'intégralité de ces informations était nécessaire à la sauvegarde des intérêts en cause****. »*

L'article 6-1 de la Loi Sapin II précise que le statut de lanceur d'alerte ainsi que les protections qui en découlent bénéficient également[7] :

- Aux facilitateurs, c'est-à-dire toute personne physique ou toute personne morale de droit privé à but non lucratif (par exemple une association ou un syndicat) qui aide un lanceur d'alerte à effectuer un signalement ou une divulgation dans le respect des dispositions de la Loi Sapin II ;
- Aux personnes physiques en lien avec le lanceur d'alerte et qui risquent de faire elles-mêmes l'objet de mesures de représailles ;
- Aux entités juridiques contrôlées (au sens de l'article L.233-3 du code de commerce) par le lanceur d'alerte et avec lesquelles il travaille ou est lié professionnellement.

Cette protection ne s'applique que si le lanceur d'alerte respecte le cadre prévu par les articles 6 à 8 de la loi n° 2016-1691 du 9 décembre 2016.

**Ces protections du lanceur d'alerte s'accompagnent de devoirs. Le lanceur d'alerte ne sera pas protégé s'il ne répond pas aux définitions légales et notamment s'il déclare des faits de mauvaise foi et/ou dont il n'aurait pas eu personnellement connaissance lorsque les informations n'ont pas été obtenues dans le cadre de son activité professionnelle. Il s'exposerait alors à des sanction civiles et pénales, notamment pour diffamation ou dénonciation calomnieuse.**

## Article 7. LES DROITS DE LA PERSONNE VISÉE PAR L'ALERTE

La personne visée par l'alerte a droit au respect de sa stricte confidentialité, notamment au regard du principe fondamental de sa présomption d'innocence et de ses droits de la défense.

Les éléments de nature à l'identifier ne peuvent être divulgués, sauf à l'autorité judiciaire, qu'une fois établi le caractère fondé de l'alerte. En d'autres termes, l'entreprise diligentera une enquête interne, étant rappelé que « *les données personnelles doivent uniquement être rendues accessibles aux personnes habilitées à en connaitre au regard de leurs attributions* ». » (Délibération de la CNIL du 18 juillet 2019), et/ou saisira l'autorité judiciaire.

La personne qui fait l'objet d'une alerte (en tant que témoin, victime ou auteur présumé des faits) doit, conformément à l'article 14 du RGPD, être informée par une alerte dans un délai raisonnable, ne pouvant pas dépasser **un mois**, à la suite de l'émission d'une alerte.

Néanmoins, conformément à l'article 14-5-b du RGPD, cette information peut être différée lorsqu'elle est susceptible « *de compromettre gravement la réalisation des objectifs dudit traitement* ». Tel pourrait par exemple être le cas lorsque la divulgation de ces informations à la personne visée compromettrait gravement les nécessités de l'enquête, par exemple en présence d'un risque de destruction de preuves. L'information doit néanmoins alors être délivrée aussitôt le risque écarté et ne doit pas contenir d'informations relatives à l'identité de l'émetteur de l'alerte ni à celle des tiers.

Toutefois, lorsqu'une sanction disciplinaire ou une procédure contentieuse est engagée à la suite de l'alerte à l'égard de la personne visée, celle-ci peut obtenir la communication de ces éléments en vertu des règles de droit commun (droits de la défense notamment).

[7] Article 2 de la loi du 21 mars 2022

ethicorp.com

Cette possibilité est néanmoins conditionnée à la prise de mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée.

L'information communiquée doit conformément à la délibération de la CNIL mentionner l'existence du traitement, ses caractéristiques (notamment les finalités poursuivies, les types de données susceptibles d'y figurer, les types de personnes susceptibles d'émettre l'alerte ou d'en faire l'objet, les principales étapes de la procédure déclenchée par l'alerte, les durées de conservation de données, etc.) ainsi que les droits dont disposent la personne visée par l'alerte.

## Article 8. DÉPÔT, TRAITEMENT ET SUIVI DE L'ALERTE – MODALITÉS PRATIQUES

La plateforme **ethicorp.com** est accessible par internet à l'adresse sécurisée **https://www.ethicorp.com**. Sauf maintenance, elle est accessible 24h/24, 7j/7, 365j/an.

Pour éviter toute inquiétude au regard de la confidentialité, il est recommandé de ne pas utiliser le matériel de l'entreprise pour se connecter.

**Création du compte de lanceur d'alerte**

Sur la plateforme, le lanceur d'alerte sera invité, avant de pouvoir déposer son alerte, à se créer un compte personnel de lanceur d'alerte.

Pour ce faire, il devra notamment renseigner le Code corporate que l'entreprise lui aura communiqué. Ce Code permet d'assurer que l'alerte est relative à l'entreprise, **ethicorp.com** ne traitant pas d'alertes relatives à des entreprises non adhérentes à ses services.

Le lanceur d'alerte devra également renseigner ses nom et prénom (sauf s'il choisit de rester anonyme, dans les conditions rappelées à l'article « **Confidentialité** »), ainsi qu'un courriel et un mot de passe.

Il est recommandé, toujours pour des questions de confidentialité, de na pas utiliser une adresse électronique professionnelle.

En toute état de cause, **ethicorp.com** conservera strictement confidentiel tout élément qui permettrait d'identifier le lanceur d'alerte, en ce compris son adresse électronique.

Après avoir validé ces informations, le lanceur d'alerte recevra un courriel ne contenant aucune donnée confidentielle, lui demandant de cliquer sur un lien internet spécifique, afin de vérifier que le courriel renseigné existe vraiment.

Une fois cette procédure achevée, le compte du lanceur d'alerte est actif, et permettra au lanceur d'alerte de déposer, consulter et compléter les alertes, ainsi que de communiquer avec les avocats d'**ethicorp.com** en toute confidentialité.

**Dépôt de l'alerte**

Le lanceur d'alerte, via son compte ouvert sur la plateforme **ethicorp.com**, peut déposer son alerte en toute confidentialité.

Il lui est demandé de décrire, en texte libre, les faits et informations dont il a été témoin personnel.

Il peut joindre des documents de nature à étayer son signalement, lorsqu'il dispose de tels éléments.

Afin de soumettre son alerte, il valide enfin sa prise de connaissance d'un avertissement détaillé lui rappelant ses droits et devoirs et l'encadrement légal d'une alerte.

Le lanceur d'alerte reçoit immédiatement un accusé de réception de son alerte, via un courriel ne contenant aucune donnée confidentielle et lui précisant l'identifiant de l'alerte.

ethicorp.com

En parallèle, l'alerte est reçue par un des avocats intervenant via la plateforme **ethicorp.com**, qui assurera son analyse et son traitement.

Le lanceur d'alerte sera informé sur son compte de lanceur d'alerte des étapes fondamentales de suivi de l'alerte : ouverture d'une enquête, d'une procédure, comme éventuellement de son classement, par exemple si les faits ne sont pas caractérisés. Cette information ne lui donnera naturellement pas accès à des informations confidentielles qui seraient obtenues dans le cadre de l'enquête ou de la procédure qui suivrait l'alerte.

Le lanceur d'alerte pourra à tout moment consulter le statut de son alerte ainsi que la préciser ou la compléter, voire déposer une autre alerte, en se connectant à son compte de lanceur d'alerte avec le courriel et le mot de passe qu'il aura renseigné à l'ouverture de son compte.

Les avocats d'**ethicorp.com** pourront avoir besoin d'entrer en contact avec le lanceur d'alerte pour lui demander de préciser son alerte, d'apporter des éléments complémentaires, ou l'informer du suivi. Le lanceur d'alerte recevra alors un courriel ne contenant aucune donnée confidentielle, lui demandant de se connecter à son compte pour prendre connaissance du message qui lui est destiné.

Le détail du fonctionnement de la plateforme avec descriptif de chaque étape figure dans le mode d'emploi que l'employeur met à la disposition des salariés et des collaborateurs externes et occasionnels.

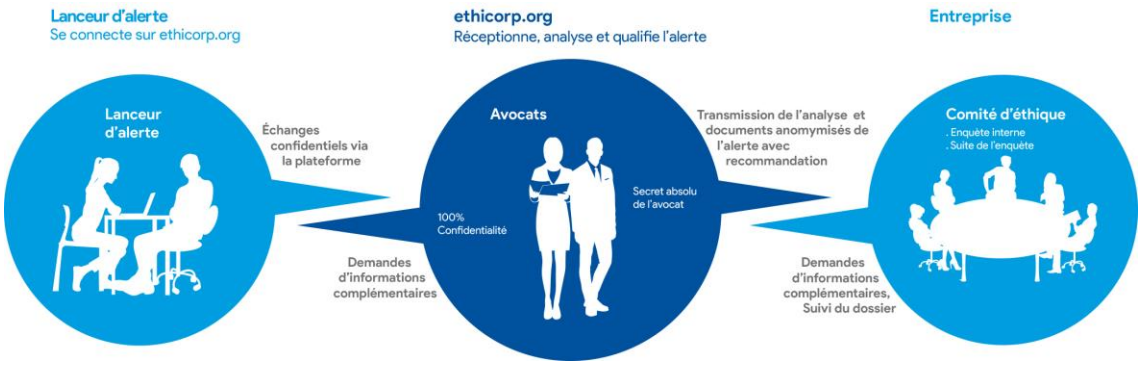
**Suites données à l'alerte**

**ethicorp.com** assure une première analyse de l'alerte, pour s'assurer qu'elle répond aux dispositions légales, notamment au regard de la gravité des faits qui peuvent être déclarés.

Si l'alerte correspond aux dispositions légales, elle est transmise (sans mention de l'identité du lanceur d'alerte) au Comité d'éthique de l'entreprise qui décidera des mesures de suivi : enquête interne, procédure judiciaire, etc.

Conformément à la délibération de la CNIL du 18 juillet 2019 « *les données personnelles doivent uniquement être rendues accessibles aux personnes habilitées à en connaitre au regard de leurs attributions* ».

Si le Comité d'éthique ou les enquêteurs ont besoin d'éléments complémentaires, **ethicorp.com** assurera l'interface avec le lanceur d'alerte afin de garantir se stricte confidentialité.




## Article 9. TRAITEMENT DES DONNÉES PERSONNELLES

La CNIL précise (délibération du 18 juillet 2019) « *que le responsable de traitement doit veiller à ce que seules les données nécessaires à la poursuite des finalités du traitement soient effectivement collectées et traitées* »

ethicorp.com

*Il lui appartient donc de s'assurer que seules les informations pertinentes et nécessaires au regard des finalités du traitement sont collectées et/ou conservées dans le dispositif d'alerte. Tel est généralement le cas des catégories suivantes :*

- *Identité, fonctions et coordonnées de l'émetteur de l'alerte ;*
- *Identité, fonctions et coordonnées des personnes faisant l'objet de l'alerte ;*
- *Identité, fonctions et coordonnées des personnes intervenant dans le recueil ou dans le traitement de l'alerte ;*
- *Faits signalés ;*
- *Éléments recueillis dans le cadre de la vérification des faits signalés ;*
- *Comptes rendus des opérations de vérification ;*
- *Suites données à l'alerte.*

Conformément à la délibération de la CNIL (18 juillet 2019) **ethicorp.com** s'est engagée notamment, par voie contractuelle, à ne pas utiliser les données à des fins détournées, à assurer leur confidentialité, à respecter la durée de conservation limitée des données et à procéder à la destruction ou à la restitution de tous les supports manuels ou informatisés de données à caractère personnel au terme de sa prestation.

L'article 8.I.C de la Loi Sapin II prévoit que lorsque la procédure de recueil et de traitement des signalements est commune à plusieurs sociétés d'un groupe, un décret fixe « *les conditions dans lesquelles des informations relatives à un signalement effectué au sein de l'une des sociétés d'un groupe peuvent être transmises à une autre de ses sociétés, en vue d'assurer ou de compléter leur traitement.* »

**Délais de conservation des données**

La conservation des données à caractère personnel est soumise aux dispositions de la loi du 6 janvier 1978 et du Règlement UE 2016/679 du parlement européen et du Conseil du 27 avril 2016 (dit Règlement Général sur la Protection des Données - RGPD), en vigueur depuis le 25 mai 2018.
Notamment, les données à caractère personnel ne peuvent être conservées que le temps strictement nécessaire à l'accomplissement de la finalité pour laquelle elles ont été collectées.

L'article 9-III de la Loi Sapin II prévoit, depuis l'entrée en vigueur de la loi du 21 mars 2022, que :

> *« Les signalements ne peuvent être conservés que le temps strictement nécessaire et proportionné à leur traitement et à la protection de leurs auteurs, des personnes qu'ils visent et des tiers qu'ils mentionnent, en tenant compte des délais d'éventuelles enquêtes complémentaires. Des données relatives aux signalements peuvent toutefois être conservées au-delà de cette durée, à la condition que les personnes physiques concernées n'y soient ni identifiées, ni identifiables.*
>
> *Lorsqu'elles font l'objet d'un traitement, les données à caractère personnel relatives à des signalements sont conservées dans le respect du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/ CE (règlement général sur la protection des données). »*

Conformément au point 7.1 du référentiel établi par la CNIL (délibération du 18 juillet 2019) :

> *« Les données relatives à une alerte considérée par le responsable du traitement comme n'entrant pas dans le champ du dispositif, sont détruites sans délai du dispositif d'alertes professionnelles ou anonymisées conformément à l'avis 05/2014 relatif aux techniques d'anonymisation du Comité européen de la protection des données (CEPD)[8].*

[8] https://www.cnil.fr/sites/default/files/atoms/files/wp216_fr_0.pdf

ethicorp.com

*Lorsqu'aucune suite*[9] *n'est donnée à une alerte rentrant dans le champ du dispositif, les données relatives à cette alerte sont détruites ou anonymisées par l'organisation chargée de la gestion des alertes, dans un délai de* ***deux mois*** *à compter de la clôture des opérations de vérification.*

*Lorsqu'une procédure disciplinaire ou contentieuse est engagée à l'encontre d'une personne mise en cause ou de l'auteur d'une alerte abusive, les données relatives à l'alerte peuvent être conservées par l'organisation chargée de la gestion des alertes* ***jusqu'au terme de la procédure ou de la prescription des recours à l'encontre de la décision.***

*A l'exception des cas où* ***aucune suite*** *n'est donnée à l'alerte, le responsable de traitement peut conserver les données collectées sous forme d'archives intermédiaires aux fins d'assurer la protection du lanceur de l'alerte ou de permettre la constatation des infractions continues. Cette durée de conservation doit être strictement limitée aux finalités poursuivies, déterminée à l'avance et portée à la connaissance des personnes concernées.*

*Les données peuvent être conservées plus longtemps, en archivage intermédiaire, si le responsable du traitement en a l'obligation légale (par exemple, pour répondre à des obligations comptables, sociales ou fiscales).*

La Commission rappelle que les décisions relatives aux suites réservées aux alertes professionnelles doivent intervenir dans un délai raisonnable à compter de l'émission de celles-ci.

Il est à préciser que la réglementation relative à la protection des données à caractère personnel ne s'applique pas, notamment en ce qui concerne les durées de conservation, aux données anonymes. Partant, le responsable du traitement peut conserver sans limitation de durée les données anonymisées. Dans ce cas, l'organisme concerné doit garantir le caractère anonymisé des données de façon pérenne.

En complément, conformément à la délibération de la CNIL du 12 février 2016 :

*Les données collectées et traitées dans le cadre de la* ***gestion d'un précontentieux*** *doivent ainsi être supprimées* ***dès le règlement amiable du litige ou, à défaut, dès la prescription de l'action en justice correspondante****.*

*Les données collectées et traitées dans le cadre d'un contentieux doivent quant à elles être supprimées* ***lorsque les voies de recours ordinaires et extraordinaires ne sont plus possibles contre la décision rendue****.*

*A l'expiration de ces périodes, les données sont supprimées de manière sécurisée ou, le cas échéant, archivées dans des conditions définies en conformité avec les dispositions du code du patrimoine relatives aux obligations d'archivage des informations du secteur public pour les organismes soumis à ces dispositions, d'une part, ou conformément aux dispositions de la délibération de la commission n° 2005-213 du 11 octobre 2005 portant adoption d'une recommandation concernant les modalités d'archivage électronique de données à caractère personnel pour les organismes relevant du secteur privé, d'autre part.*

[9] Conformément au référentiel du la CNIL du 18 juillet 2019 l'expression « *suites* » désigne toute décision prise par l'organisme pour tirer des conséquences de l'alerte. Il peut s'agir de l'adoption ou de la modification des règles internes (règlement interne, charte éthique, etc.) de l'organisme, d'une réorganisation des opérations ou des services de la société, du prononcé d'une sanction ou de la mise en œuvre d'une action en justice.

ethicorp.com

*A cet égard, la commission estime que les décisions prononcées peuvent être conservées par le responsable de traitement à titre d'archive définitive en raison d'un intérêt historique. »*

**Respect des droits d'accès et de rectification**

Les personnes concernées disposent des droits suivants, qu'ils exercent dans les conditions prévues par le RGPD :

- Droit de s'opposer au traitement de leurs données, sous réserve des conditions d'exercice de ce droit en application des dispositions de l'article 21 du RGPD ;
- Droit d'accès, de rectification et d'effacement des données qui les concernent ;
- Droit à la limitation du traitement. Par exemple, lorsque la personne conteste l'exactitude de ses données, celle-ci peut demander à l'organisme, le gel temporaire du traitement de ses données, le temps que celui-ci procède aux vérifications nécessaires.

Lorsque les personnes concernées exercent leur droit d'accès, elles ne peuvent via l'exercice de ce droit, obtenir communication d'aucune donnée relative à des tiers.

La personne visée par l'alerte qui exercerait son droit d'accès ne peut en aucun cas obtenir communication des informations concernant l'identité de l'émetteur de l'alerte.

Conformément à l'article 21 du RGPD, le droit d'opposition ne peut pas être exercé pour les traitements nécessaires au respect d'une obligation légale à laquelle est soumis le responsable du traitement (notamment concernant les traitements mis en place par des sociétés remplissant les conditions des articles 8 et/ou 17 de la Loi Sapin II).

En revanche, lorsqu'un organisme se dote d'un dispositif d'alertes sur une base purement volontaire, le droit d'opposition existe. Partant, les personnes concernées devront être informées de son existence et le responsable du traitement devra veiller à en assurer le respect.

Toutefois, l'exercice de ce droit n'est pas automatique : la personne qui l'exerce doit caractériser l'existence de « raisons tenant à sa situation particulière ».

Le responsable du traitement devra prendre en compte l'opposition, sauf à démontrer :

- Qu'il existe des motifs légitimes et impérieux qui prévalent sur les intérêts et les droits et intérêts de la personne concernée ;
- Ou que le traitement est nécessaire pour la constatation, l'exercice ou la défense de droits en justice

Enfin la CNIL (délibération du 18 juillet 2019) précise que le droit de rectification, prévu à l'article 16 du RGPD, doit s'apprécier au regard de la finalité du traitement.

Ce droit de rectification est limité et ne peut pas permettre la modification rétroactive des éléments contenus dans l'alerte ou collectés lors de son instruction. Son exercice, lorsqu'il est admis, ne doit pas aboutir à l'impossibilité de reconstitution de la chronologie des éventuelles modifications d'éléments importants de l'enquête.

Ce droit ne peut être exercé uniquement pour rectifier les données factuelles, dont l'exactitude matérielle peut être vérifiée par le responsable du traitement à l'appui d'éléments probants, et ce sans que soient effacées ou remplacées les données, même erronées, collectées initialement.

Pour toute demande, s'adresser à la SAS ethicorp.com, 7 rue Royale, 75008 Paris, contact@ethicorp.com

ethicorp.com

### Article 10. DIFFUSION DE LA PRÉSENTE PROCÉDURE - INFORMATION

Conformément au décret du 19 avril 2017, *« L'organisme procède à la diffusion de la procédure de recueil des signalements qu'il a établie par tout moyen, notamment par voie de notification, affichage ou publication, le cas échéant sur son site internet, dans des conditions propres à permettre à la rendre accessible aux membres de son personnel ou à ses agents, ainsi qu'à ses collaborateurs extérieurs ou occasionnels. Cette information peut être réalisée par voie électronique. »*

Les Recommandations de l'Agence française anticorruption rappellent également que les différentes étapes de la mise en œuvre du dispositif d'alerte devraient comporter la « *diffusion de la procédure d'alerte interne à l'ensemble des personnels par tous moyens (courrier de la direction, affichage, site intranet, remise en main propre, etc.) permettant de s'assurer que chaque personne concernée en a connaissance et y a accès. Dans le cas d'un dispositif d'alerte commun à l'alerte anticorruption et à d'autres dispositifs légaux, la procédure doit être également diffusée aux collaborateurs occasionnels. L'entreprise peut décider d'ouvrir son dispositif d'alerte aux tiers. L'entreprise peut choisir de mettre à profit ses outils de communication externes pour mentionner l'existence de son dispositif d'alerte (par exemple son site internet, les documents remis à ses tiers, etc.) ;* »

Par ailleurs, la CNIL (délibération du 18 juillet 2019) recommande que l'ensemble des personnes potentiellement concernées par le dispositif en soient informées préalablement à son introduction dans l'organisme.

Cette information précise le fonctionnement du dispositif, notamment les étapes de la procédure de recueil des signalements, et en particulier les destinataires et les conditions auxquelles l'alerte peut leur être adressée.

Le responsable de traitement indique expressément que l'utilisation abusive du dispositif peut exposer son auteur à des sanctions ou des poursuites mais qu'à l'inverse, l'utilisation de bonne foi du dispositif n'exposera son auteur à aucune sanction disciplinaire, quand bien même les faits s'avéreraient par la suite inexacts ou ne donneraient lieu à aucune suite.

Le responsable de traitement rappelle que le dispositif d'alerte n'est qu'un moyen de signalement parmi d'autres (comme peut l'être la voie hiérarchique), et que le fait de ne pas y avoir recours ne peut entrainer aucune sanction à l'encontre des membres du personnel.

Enfin il est recommandé que l'information individuelle des personnes soit privilégiée dans la mesure du possible.

### Article 11. FORMATION DU PERSONNEL

Conformément aux Recommandations de l'Agence française anticorruption :

- *« L'entreprise veille à la formation des personnes en charge du traitement de l'alerte, au respect de la confidentialité de son traitement et à l'absence de tout conflit d'intérêts ; elle veille également à la formation des supérieurs hiérarchiques. » (§258)*
- *« Le dispositif d'alerte interne est présenté sans délai aux collaborateurs venant de rejoindre l'entreprise. » (§259)*
- Les différentes étapes de la mise en œuvre du dispositif d'alerte devraient comporter :
    - La « *présentation du dispositif d'alerte dans le cadre des actions de sensibilisation de l'ensemble des personnels ;* »
    - La « *formation des personnels amenés à recueillir, gérer et traiter les alertes, notamment sur les obligations de confidentialité, et formation des personnels les plus exposés* ».

FAIT A VELIZY-VILLACOUBLAY, le 13/11/2022