DISPOSITIF D'ALERTE INTERNE

↘ Le présent dispositif d'alerte interne est instauré en application de la loi Sapin 2. Il est un outil d'amélioration continu du dispositif de conformité du Groupe.

↘ Le dispositif d'alerte interne est ouvert aux Collaborateurs du Groupe ainsi qu'aux tiers prévus par la loi.

↘ Le dispositif définit les modalités de dépôt d'une alerte, qui peut se faire via le canal hiérarchique classique ou via la plateforme d'alerte éthique ETHICORP, externalisée et gérée par des avocats, en cliquant sur le lien suivant : www.ethicorp.com/gorgegroup.

↘ Le dispositif définit les modalités et les principes généraux de traitement d'une alerte.

↘ Le lanceur d'alerte répondant aux critères légaux bénéficie de nombreuses protections. Sauf exception, son identité restera confidentielle tout au long du traitement de l'alerte. Cette confidentialité couvre également les personnes visées par l'alerte et les faits objet de l'alerte.

↘ Une utilisation abusive ou de mauvaise foi du dispositif d'alerte, de même que le non-respect des obligations de confidentialité ou le fait de prendre contre un lanceur d'alerte des mesures de représailles sont passibles de sanctions.

SOMMAIRE

1. INTRODUCTION

1.1 CHAMP D'APPLICATION

Le présent dispositif d'alerte est adopté en application de la loi n° 2016-1691 du 9 décembre 2016 dite loi Sapin 2, telle que modifiée.

Il s'applique à Gorgé SAS et sa filiale Exail Technologies SA ainsi qu'à l'ensemble de leurs filiales françaises et étrangères (ensemble le « Groupe») se référant à ce dispositif d'alerte.

Toutes les entités du Groupe sont invitées à adopter ce dispositif d'alerte interne ou un dispositif similaire conforme à la réglementation. Il sera alors annexé à leur règlement intérieur après consultation des IRP et diffusé en interne à tous les Collaborateurs, par tout moyen (affichage, envoi, intranet, etc.), et ce conformément au décret 2022-1284 du 2 octobre 2022.

Tout salarié ou collaborateur externe ou occasionnel du Groupe (ensemble les « Collaborateurs »), de même que tout tiers désigné au Chapitre 3.1 de la présente politique doit pouvoir déposer une alerte conformément aux stipulations du Chapitre 4 et bénéficier des protections au titre du statut de lanceur d'alerte rappelées au Chapitre 3.3 sous réserve de respecter les conditions prévues au Chapitre 3.2.

À cette fin, Gorgé SAS et sa filiale Exail Technologies ont choisi de mettre en place, pour elles-mêmes et pour l'ensemble de leurs filiales non dotées de leur propre dispositif d'alerte, le dispositif d'alerte éthique ETHICORP qui permet de recueillir, sur une plateforme externalisée et gérée par des avocats, tout signalement répondant aux conditions de la présente politique. Le lien est le suivant : www.ethicorp.com/gorgegroupPour les salariés du Groupe, ce dispositif ETHICORP est complémentaire des autres canaux internes mis à leur disposition, et notamment le canal hiérarchique ou le canal des ressources humaines ou de la direction juridique de leur entité. L'utilisation de la plateforme ETHICORP ne constitue qu'une faculté supplémentaire offerte à tout Collaborateur.

1.2 OBJECTIFS DU DISPOSITIF D'ALERTE INTERNE

Le Groupe considère que la remontée d'informations à travers le canal de l'alerte interne permet la détection de signaux faibles de problématiques pouvant affecter, de façon potentiellement grave, le fonctionnement, la réputation ou la performance du Groupe.

C'est donc un outil d'amélioration continue à part entière. C'est dans ce sens que les Collaborateurs du Groupe sont invités à s'en saisir, dans le respect de la présente politique.

1.3 RAPPEL DES TROIS CANAUX DE SIGNALEMENT PREVUS PAR LA LOI

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 :

i. **Signalement interne** : le lanceur d'alerte choisit de déposer l'alerte en interne via le dispositif d'alerte éthique ETHICORP ou directement auprès de toute autre personne habilitée – c'est l'objet de la présente politique.

ii. **Signalement externe** : le lanceur d'alerte peut adresser son alerte à toute autorité compétente telle que listée en annexe du décret n° 2022-1284 du 3 octobre 2022, ou encore au Défenseur des droits, à l'autorité judiciaire ou à toute institution, organe ou organisme de l'Union européenne compétent. Ce signalement externe peut intervenir soit après un signalement interne, soit directement lorsque le lanceur d'alerte estime qu'il n'est pas possible de remédier efficacement à la situation par un signalement interne ou qu'il s'expose à un risque de représailles.

iii. **Divulgation publique** : le lanceur d'alerte peut enfin rendre l'alerte publique dans certaines conditions précises :
   - soit après signalement externe et dans la mesure où celui-ci n'a été suivi d'aucune mesure appropriée dans les délais fixés ;
   - soit en cas de danger grave et imminent ;
   - soit enfin 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, en raison des circonstances particulières de l'affaire.

Le Dispositif d'alerte éthique mis en place par le Groupe porte exclusivement sur le signalement interne visé au (i) ci-dessus.

1.4 DIFFUSION DE LA PRESENTE POLITIQUE

La présente politique doit faire l'objet d'une diffusion par tous moyens (courrier de la direction, affichage, e-mail, site intranet, remise en main propre, etc.) auprès de l'ensemble des Collaborateurs du Groupe.

Elle doit être adoptée et annexée au règlement intérieur des entités concernées afin que chacun puisse s'y référer.

Elle est en outre rendue accessible aux tiers via le site internet de Gorgé SAS (www.gorge-entreprises.com) et de Exail Technologies (www.exail-technologies.com).

2. *L'OBJET DE L'ALERTE*

Conformément à la loi Sapin 2, le présent dispositif répond au double objectif suivant :

1. **Recueil des alertes anti-corruption**[1] : dans le cadre de la prévention et de la détection des faits de corruption et de trafic d'influence en France et à l'étranger auxquels le Groupe pourrait être confronté, chaque salarié des filiales du Groupe peut signaler d'éventuelles conduites contraires au Code de conduite anti-corruption de Gorgé SAS et de Exail Technologies SA, qui s'applique à l'ensemble des entités du Groupe, ou à toute autre politique ou procédure interne en découlant.

2. **Recueil des alertes générales de faits très graves**[2] : tout salarié et tout collaborateur extérieurs ou occasionnels (stagiaire, intérimaire, prestataire, sous-traitant) des filiales de Gorgé SAS ou Exail Technologies SA peut signaler des éventuel(le)s :
   - violation des politiques ou procédures internes du Groupe ;
   - crime ou délit ;
   - infractions boursières (notamment manquements à l'article L.634-1 du Code monétaire et financier) ;
   - violation grave et manifeste d'un engagement régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale prise sur le fondement d'un tel engagement, de la loi ou du règlement ;
   - atteintes envers les droits humains et les libertés fondamentales, la santé et la sécurité des personnes ainsi que l'environnement ;
   - menace ou préjudice grave pour l'intérêt général.

En revanche, le lanceur d'alerte ne peut révéler d'informations couvertes par :

- le secret de la Défense Nationale ;
- le secret médical ;
- le secret des délibérations judiciaires ;
- le secret de l'enquête ou de l'instruction judiciaire ; ou
- le secret des relations entre un avocat et son client.

Les informations peuvent porter sur des faits susceptibles de se produire ou s'étant déjà produits.

En cas de doute, il est préférable d'utiliser le dispositif d'alerte interne plutôt que de prendre le risque qu'un fait grave ou sous-estimé ne soit pas révélé.

[1] Conformément à l'article 17 de la Loi Sapin 2.
[2] Conformément à l'article 6 de la Loi Sapin 2.

3. *LE STATUT DE LANCEUR D'ALERTE*

3.1 QUI PEUT LANCER UNE ALERTE

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.

3.2 LES CONDITIONS DU STATUT DE LANCEUR D'ALERTE

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 ;
- agissant **sans contrepartie financière directe** – en France le lanceur d'alerte n'est pas rémunéré ;
- et **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.

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.

3.3 LES PROTECTIONS ET DEVOIRS DU LANCEUR D'ALERTE

Conformément aux dispositions de la loi Sapin 2, telle que modifiée par la loi du 21 mars 2022 et complétée par le décret du 3 octobre 2022, dès lors que le lanceur d'alerte respecte les conditions visées au paragraphe 1.2 ci-dessus, celui-ci bénéfice d'une large protection et notamment des garanties suivantes :

- Confidentialité des données le concernant, qui ne peuvent être divulguées sans son consentement[3] ;
- Toute mesure de représailles, directe ou indirecte, à l'encontre d'un lanceur d'alerte ne saurait être tolérée (telles que suspension, licenciement, mesure disciplinaire, discrimination, traitement désavantageux…), étant précisé que dans ce cadre un aménagement de la charge de la preuve est prévu : il appartient au Groupe de prouver que sa potentielle décision de licencier ou de sanctionner une personne à l'origine d'une alerte est motivée par des éléments objectifs étrangers à l'alerte ;
- Irresponsabilité pénale et civile (notamment si le lanceur d'alerte avait des motifs raisonnables de croire, au moment du signalement, que celui-ci était nécessaire à la sauvegarde des intérêts en cause).

Conformément à l'article 2 de la loi du 21 mars 2022, le statut protecteur du lanceur d'alerte bénéficie également :

- 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 ;
- Aux personnes physiques en lien avec le lanceur d'alerte (par exemple des collègues ou des proches) et qui risque de faire elles-mêmes l'objet de mesures de représailles de la part de leur employeur, de leur client ou du destinataire de leurs services ;
- 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 Sapin 2.

[3] Sauf si le Groupe décidait de communiquer ces faits à l'autorité judiciaire.

Afin d'encourager le dépôt d'alertes internes et de protéger les lanceurs d'alertes, la loi réprime un certain nombre de manquements aux exigences posées :

- 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 pour les personnes physiques (art. 13, I. de la loi Sapin 2) ;
- Toute violation de la confidentialité de l'alerte, du lanceur d'alerte, de la personne visée par l'alerte ou de personnes mentionnées dans l'alerte est punie de deux ans d'emprisonnement et 30.000 euros d'amende, 150.000 euros pour les personnes morales (art. 9, II. de la loi Sapin 2) ;
- Toute discrimination fondée sur la « *qualité de lanceur d'alerte, de facilitateur ou de personne en lien avec un lanceur d'alerte* » est punie de trois ans d'emprisonnement et de 45.000 euros d'amende (art. 225-1 et 225-2 du Code pénal) ;
- En outre, les procédures dilatoires ou abusives inventées contre un lanceur d'alerte peuvent être sanctionnées par une amende civile de 60.000 euros, sans préjudice de l'octroi de possibles dommages et intérêts ainsi que le prononcé d'une peine de diffusion de la décision (art. 13, II. de la loi Sapin 2).

Les amendes prévues pour les personnes physiques sont multipliées par cinq pour les personnes morales.

Ces protections du lanceur d'alerte s'accompagnent de devoirs.

Le lanceur d'alerte est lui-même soumis à une obligation de confidentialité concernant l'identité des personnes visées dans l'alerte (mises en cause, victimes ou témoins par exemple), comme rappelé au Chapitre 3.4 *infra*. Le lanceur d'alerte ne saurait en conséquence, en dehors des échanges intervenant dans le cadre du traitement de l'alerte, divulguer des informations permettant de les identifier, sous peine de sanctions pénales (deux ans d'emprisonnement et 30.000 euros d'amende).

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 sanctions civiles et pénales, notamment pour diffamation ou dénonciation calomnieuse.

En revanche, toute utilisation de bonne foi du dispositif d'alerte éthique, même si les faits se révèlent, par la suite, inexacts ou ne donnent lieu à aucune suite, ne peut exposer son auteur à des sanctions ou des représailles.

3.4 LES DROITS DES PERSONNES VISEES 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.

Cela concerne les personnes mises en cause comme les personnes pouvant être citées comme témoins, victimes ou être autrement visées dans l'alerte.

Cette obligation de confidentialité s'impose au Groupe et à ses représentants habilités, qui recueillent l'alerte, comme au lanceur d'alerte et à toute personne qui serait ensuite entendue dans le cadre d'une enquête interne.

Cette obligation de confidentialité est sanctionnée pénalement (deux ans d'emprisonnement et 30.000 euros d'amende).

Les éléments de nature à identifier les personnes visées par l'alerte 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 accessibles aux personnes habilitées à en connaitre au regard de leurs attributions* ». (Référentiel CNIL du 6 juillet 2023), 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 confirmée.

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 suite à 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).

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.

↘ Le lanceur d'alerte est une personne physique, agissant de bonne foi et sans contrepartie directe.

↘ Le dépôt d'une alerte est ouvert aux salariés, collaborateurs externes ou occasionnels, et anciens salariés mais également à de nombreux tiers qui ont pu interagir avec le Groupe.

↘ Dès lors qu'il répond aux conditions posées par la loi, le lanceur d'alerte ainsi que les éventuels facilitateurs bénéficient d'un certain nombre de protections (confidentialité, irresponsabilité civile et pénale, absence de mesures de représailles).

↘ Les personnes visées par l'alerte ont également droit au respect de la confidentialité de leur identité, notamment au regard de la présomption d'innocence et du respect des droits de la défense, sauf exception.

4. *COMMENT DEPOSER UNE ALERTE*

4.1 LE DEPOT D'UNE ALERTE SUR LA PLATEFORME ETHICORP

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

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

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

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

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

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 email ne contenant aucune donnée confidentielle et lui précisant l'identifiant de l'alerte.

En parallèle, l'alerte est reçue par un des avocats intervenant via la plateforme **ethicorp.com**, lequel 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 l'email 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 email 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.

4.2 LE DEPOT D'UNE ALERTE À TRAVERS LA VOIE HIERARCHIQUE OU AUPRES DES REFERENTS

Avant de lancer une alerte, chaque Collaborateur pourra – s'il le souhaite – s'adresser à son supérieur hiérarchique ou à toute personne visée dans les points de contact du Code de conduite anti-corruption du groupe ou de sa filiale, ce dernier ayant pour devoir de l'orienter et le conseiller.

Le(s) Référent(s) est(sont) chargé(s) de recueillir et traiter les alertes :

- Qui leur sont adressées ;
- qui sont adressées à la hiérarchie directe du lanceur d'alerte.

Les Référents nommés par le Président de Gorgé SAS sont :

- la Directrice juridique de Gorgé SAS et Exail Technologies SA et
- le Directeur Administratif et Financier de Gorgé SAS et Exail Technologies SA.

4.3 CONTENU DE L'ALERTE

Quel que soit le canal choisi par le lanceur d'alerte, les échanges peuvent se faire sous toutes formes, par écrit (y compris par e-mail) ou par oral et, le cas échéant, lors d'une visioconférence ou d'une rencontre physique organisée au plus tard vingt jours ouvrés après la réception de la demande. En tout état de cause, la confidentialité de cet échange doit être assurée par la personne qui recueille l'alerte comme par le lanceur d'alerte (voir Chapitres 3.4 ci-dessus et 6 ci-dessous).

Afin de pouvoir être traitée, il est recommandé au lanceur d'alerte:

- De rédiger l'alerte en langue française ou anglaise ;

- D'indiquer son identité et ses coordonnées ;

Le lanceur d'alerte peut indiquer son identité. Cela évite des dénonciations calomnieuses ou infondées et permet de demander le cas échéant des informations au lanceur d'alerte. Son identité sera protégée par les avocats ethicorp ou les Référents et le Comité éthique selon le cas.

Toutefois le lanceur d'alerte peut, s'il le souhaite, rester anonyme lorsque (i) la gravité des faits mentionnés est établie, (ii) les éléments factuels relatifs à l'alerte sont suffisamment détaillés et (iii) si le traitement de ce signalement permet de s'entourer de précautions particulières. Si ces conditions ne sont pas réunies, le lanceur d'alerte sera invité à s'identifier pour que son alerte puisse être traitée.

- D'indiquer l'identité et les fonctions de la personne faisant l'objet du signalement ;
- D'énoncer les faits signalés ;
- De joindre des documents de nature à étayer son signalement, lorsqu'il en dispose ;
- De ne pas utiliser son matériel professionnel (ordinateur, tablette, téléphone professionnel) afin de déposer son alerte ;
- De renseigner une adresse mail sur laquelle il pourra être joint dans le cadre du traitement de l'alerte. Afin de garantir la confidentialité de son identité, cette adresse mail pourra utiliser un pseudo.

Le signalement doit être précis et accompagné d'éléments de preuve (courriers, rapports, documents comptables, etc.).

Ces éléments permettront ensuite aux avocats de la plateforme ethicorp ou aux Référents et au Comité éthique selon le cas, d'analyser et d'enquêter sur les faits rapportés.

5. LE TRAITEMENT DE L'ALERTE

5.1 RECEPTION DE L'ALERTE

A la suite d'un signalement, le lanceur d'alerte recevra un accusé réception du signalement dans un délai de sept jours. Cet accusé de réception ne préjuge aucunement de la recevabilité éventuelle de l'alerte, ce point étant analysé dans un second temps. Il sera également informé des modalités suivant lesquelles il sera tenu au courant des suites données à son signalement.

Au cours du traitement de l'alerte, l'auteur du signalement pourra transmettre toute information et document complémentaire (via la plateforme ethicorp le cas échéant, ou à défaut par écrit/oral, par e-mail ou remise en main propre).

5.2 ANALYSE ET TRAITEMENT DE L'ALERTE

➢ **En cas de dépôt d'une alerte sur la plateforme ethicorp**

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) aux Référents qui décideront des mesures de suivi : enquête interne, procédure judiciaire, constitution d'un Comité éthique, etc.

Conformément au Référentiel CNIL du 6 juillet 2023 « *les données personnelles doivent uniquement être accessibles aux personnes habilitées à en connaitre au regard de leurs attributions* ».

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

➢ **En cas de dépôt d'une alerte via le canal hiérarchique interne**

A réception d'un signalement, les Référents en sont informés sans délai et :

- analysent le caractère sérieux des faits allégués et la recevabilité *prima facie* de l'alerte ;
- procèdent le cas échéant à des vérifications élémentaires ;
- après examen du caractère sérieux des faits invoqués et de la précision des informations données, les Référents statuent sur la recevabilité de l'alerte et, le cas échéant, les suites qu'ils doivent donner (enquête interne, procédure judiciaire…) ainsi que les mesures de remédiation pouvant être mise en œuvre.

Si l'alerte est jugée recevable, les Référents, en fonction de l'objet du signalement reçu, peuvent à leur discrétion, :

- déléguer le traitement de l'alerte à des avocats ou consultants extérieurs ; ou

- former un **Comité éthique**, pour décider du traitement des signalements. Ce Comité sera composé dans tous les cas des Référents, qui pourront s'adjoindre des compétences supplémentaires tel que;
    - Un expert informatique interne ou externe ;
    - Des référents des autres filiales du groupe ;
    - Un avocat ;
    - Tout spécialiste interne ou externe au groupe dont l'expertise est nécessaire au traitement d'une alerte ;
    - En cas de difficultés particulières (importance des sujets, personnes impliquées, …) une remontée à la direction générale de la filiale concernée et aux Dirigeants du Groupe est organisée.

La composition de ce Comité éthique dépendra des alertes et des expertises requises au cas par cas. Les Référents veilleront à ce que ce Comité ne comporte pas de personnes en position de conflit d'intérêt dans le cadre d'une alerte donnée.

Chaque membre du Comité éthique sera amené à signer une Charte éthique qui rappellera (i) les principes généraux régissant les alertes internes, (ii) les modalités de conduite des enquêtes internes, (iii) les obligations de confidentialité, neutralité et d'impartialité à respecter en toutes circonstances par les membres du Comité.

Le Comité éthique traitera les alertes transmises par les Référents.

Au regard des circonstances (si les faits sont suffisamment étayés ou non), les Référents ou le Comité éthique pourront décider ou non de diligenter eux-mêmes ou contribuer à une enquête interne (recherche de preuves, recherches informatiques, auditions de personnes, etc.) ou d'en déléguer et superviser la réalisation afin de déterminer la réalité et la matérialité des faits signalés.

Le cas échéant, des échanges préservant la confidentialité de l'identité du lanceur d'alerte pourront être organisés avec ce dernier.

Le Comité éthique informe les personnes visées par le signalement, sauf en cas de mesure conservatoire pour la collecte de preuves à mettre en œuvre au préalable. En effet, toute personne visée par une alerte, que ce soit en tant que témoin, victime ou auteur présumé des faits doit en être informée dans un délai raisonnable, lequel ne peut dépasser un mois à la suite de l'émission de l'alerte, sauf à ce que cette information soit susceptible « *de compromettre gravement la réalisation des objectifs dudit traitement* », tel le risque de destruction de preuves[4]. L'information doit néanmoins alors être délivrée aussitôt le risque écarté et ne doit pas contenir d'informations relatives à l'identité de l'auteur de l'alerte ni à celle de toute autre personne visée par l'alerte. L'information donnée devra mentionner l'existence du traitement, ses caractéristiques ainsi que les droits dont dispose la personne visée par l'alerte. Il sera également précisé à cette personne les faits qui lui sont reprochés, les services éventuellement destinataires du signalement, les modalités d'exercice de ses droits d'accès et de rectification.

L'identité de l'auteur du signalement ne pourra ne aucun cas lui être communiquée.

En outre, les éléments de nature à identifier la personne mise en cause par l'alerte ne peuvent être divulgués, sauf à l'autorité judiciaire, qu'une fois établi le caractère fondé de l'alerte. En d'autres termes,

[4] Articles 14 et 14-5-b du Règlement Général sur la Protection des Données (« **RGPD** »).

dans le cadre du traitement de l'alerte par les Référents et les éventuels autres membres du Comité éthique, « *les données personnelles doivent uniquement être rendues accessibles aux personnes habilités à en connaître au regard de leurs attributions* »[5], sauf à devoir saisir l'autorité judiciaire.

5.3 RESOLUTION - SUITES DONNEES A L'ALERTE

A l'issue de l'examen de l'alerte par les Référents ou le Comité éthique, quelle que soit l'issue donnée à l'alerte, la décision des Référents ou du Comité éthique sera formalisée dans un document.

En cas d'enquête, un rapport d'enquête interne est établi et adressé aux Référents, au Comité éthique et/ou à l'instance dirigeante selon le cas.

L'auteur du signalement sera tenu informé des suites données à son signalement dans un délai de trois mois à compter de l'accusé de réception. Il est également tenu informé de la clôture du dossier lié à son signalement.

La personne mise en cause par l'alerte sera informée de la clôture des opérations de vérification, le cas échéant, ou de la mise en œuvre d'une procédure disciplinaire ou de poursuites judiciaires.

Dès lors qu'une sanction disciplinaire ou une procédure contentieuse est engagée à la suite de l'alerte à l'encontre de la personne mise en cause, cette dernière pourra obtenir communication de certains éléments de son dossier en vertu des règles de droit commun applicables, en ce compris l'identité du lanceur d'alerte et de toute autre personne visée par l'alerte, sous réserve toutefois de la prise de mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes des personnes concernées.

5.4 PRINCIPES FONDAMENTAUX DE TRAITEMENT DE L'ALERTE

Tout signalement sera traité par les avocats d'ethicorp, de même que les Référents et le Comité éthique selon le cas, dans le respect des principes fondamentaux suivants :

- discrétion et confidentialité ;
- objectivité et impartialité ;
- présomption d'innocence des personnes visées par l'alerte, principe du contradictoire et respect des droits de la défense ;
- respect de la vie privée et du RGPD ;
- loyauté et proportionnalité.

6. CONFIDENTIALITE ET PROTECTION DES DONNEES PERSONNELLES

[5] Délibération de la CNIL du 18 juillet 2019.

6.1 GESTION DE LA CONFIDENTIALITE

Toute personne visée par une alerte (témoin, victime, auteur présumé) a droit au strict respect de sa confidentialité, notamment au regard du principe fondamental de la **présomption d'innocence**, du respect des **droits de la défense** et du **respect de la vie privée**. Au titre du RGPD, elle doit être informée qu'elle est visée par une alerte, ces données personnelles faisant l'objet d'un traitement à ce titre.

Gorgé SAS ou Exail Technologies SA, selon le cas, est responsable de traitement en cas d'alerte[6].

La CNIL précise dans son Référentiel du 6 juillet 2023 que « *le référent ou prestataire de service (…)* [à savoir ici ethicorp] *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 (…)* ».

Le lanceur d'alerte ne peut pas lui-même divulguer librement les informations objet de l'alerte.

Le respect de la confidentialité étant l'un des principes fondamentaux de traitement d'une alerte, il est rappelé que l'identité du lanceur d'alerte ne sera pas communiquée à la (les) personne(s) mise(s) en cause dans l'alerte, sauf accord du lanceur l'alerte.

Lors du traitement d'une alerte, seules les informations suivantes seront enregistrées :

- L'identité, fonctions et coordonnées du lanceur d'alerte, des personnes faisant l'objet de l'alerte, des personnes intervenant dans le recueil ou dans le traitement de l'alerte ;
- Les faits signalés ;
- Les éléments recueillis dans le cadre de la vérification des faits signalés ;
- Le compte rendu des opérations de vérification ;
- Les suites données à l'alerte.

La prise en compte du signalement s'appuie sur des données formulées de manière objective, par exemple, des dates, des noms et des fonctions internes des personnes impliquées, en rapport direct avec l'objet du dispositif d'alerte interne et strictement nécessaires à la vérification des faits allégués.

La réception, le traitement et le classement d'une alerte seront traités de manière confidentielle, sous réserve des obligations découlant de la loi ou des procédures judiciaires applicables. Des mécanismes spécifiques ont ainsi été mis en place afin de garantir une stricte confidentialité de : (i) l'identité des lanceurs d'alerte ; (ii) l'identité des personnes visées par l'alerte ; et (iii) des informations recueillies par l'ensemble des destinataires du signalement. Ces mécanismes comprennent notamment la mise en place : (i) d'une adresse mail dont l'accès est restreint aux seuls Référents, (ii) d'un espace de stockage (ou Cloud) hébergé localement et dont l'accès aux serveurs est sécurisé, (iii) d'une Charte éthique signée par les membres du Comité éthique (y compris les Référents) les informant des sanctions applicables en cas de violation de la confidentialité ; (iii) d'accords de confidentialité avec tout tiers lorsque la

[6] Lorsqu'elles font l'objet d'un traitement, les données à caractère personnel relatives à des signalements sont traitées et 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 des données.

vérification ou le traitement d'une alerte nécessitera une expertise externe ; et (iv) de modalités de destruction ou archivage des données.

La confidentialité pourra être levée dans les cas suivants :

- Divulgation de l'identité du lanceur d'alerte avec son consentement ;
- Divulgation de la personne mise en cause par l'alerte une fois le caractère fondé de l'alerte établi. A ce sujet, et conformément au Référentiel de la CNIL du 6 juillet 2023, « *les données personnelles doivent uniquement être accessibles aux personnes habilitées à en connaître au regard de leurs attributions* » ;
- transmission à l'autorité judiciaire.

6.2 PROTECTION DES DONNEES A CARACTERE PERSONNEL

Toute donnée à caractère personnel communiquée en application du présent dispositif d'alerte interne sera traitée conformément aux dispositions légales applicables en matière de protection et traitement des données à caractère personnel.

Les destinataires de tout ou partie des données sont les personnes habilitées à recueillir une alerte ainsi que les membres du Comité éthique, sous réserve des limitations liées à la préservation de la confidentialité entourant l'identité du lanceur d'alerte.

Ces données sont collectées dans le but de se conformer à la loi Sapin 2, et plus généralement aux obligations légales applicables à Gorgé SAS et Exail Technologies SA. Elles seront enregistrées dans un fichier informatisé, pourront être transmises selon le cas aux avocats ethicorp, aux Référents, aux membres du Comité éthique ainsi qu'aux autorités administratives et judiciaires compétentes.

La durée de conservation de ces données 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 (RGPD), en vigueur depuis le 25 mai 2018.

Conformément au point 7.1 du Référentiel de la CNIL du 6 juillet 2023 :

- les données relatives à une alerte peuvent être conservées en base active jusqu'à la prise de la décision définitive sur les suites à réserver à celle-ci. Cette décision doit intervenir dans un délai raisonnable à compter de la réception du signalement ;

- après la prise de décision définitive sur les suites à réserver à l'alerte, les données pourront être conservées sous forme d'archives intermédiaires, « *le temps strictement 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* » ;

- 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 le Comité éthique jusqu'au terme de la procédure ou de la prescription des recours à l'encontre de la décision intervenue.

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), ou à des fins probatoires dans l'optique d'un contrôle ou d'un contentieux éventuel, ou encore à des fins de réalisation des audits de qualité des processus de traitement des signalements.

En outre, et conformément à la délibération de la CNIL du 14 janvier 2016, « *les données traitées pour gérer un précontentieux doivent être supprimées dès le règlement amiable du litige ou, à défaut, dès la prescription de l'action en justice correspondante. Les données traités pour gérer un contentieux doivent être supprimées lorsque les recours ne sont plus possibles contre la décision rendue pour la faire exécuter* ».

L'émetteur de l'alerte et la personne faisant l'objet de l'alerte peuvent à tout moment accéder aux données les concernant et en demander, si elles sont inexactes, incomplètes, équivoques ou périmées, la **rectification** ou la **suppression**.

Lorsque les personnes concernées exercent leur droit d'accès, elles ne peuvent via l'exercice de ce doit, obtenir communication d'aucune donnée relative à des tiers. En particulier, la personne par l'alerte qui exercerait son droit d'accès ne peut en aucun cas obtenir communication des informations concernant l'identité de l'auteur de l'alerte.

Conformément au Référentiel de la CNIL du 6 juillet 2023, 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 limitée 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 faits ni à d'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 exercer ce droit, il convient de s'adresser à la Direction juridique de Gorgé SAS ou Exail Technologies SA, selon le cas, à l'adresse suivante : compliance@groupe-gorge.com.