

Procédure de recueil et de traitement des signalements

France / Corporate



Procédure de recueil et de traitement des signalements

France / Corporate

01. OBJECTIFS	3
02. CHAMP D'APPLICATION	3
03. QUI PEUT ÉMETTRE UN SIGNALEMENT ?	5
04. QUELS TYPES D'ACTES OU DE COMPORTEMENTS PEUT-ON SIGNALER ?	5
05. LES RÉFÉRENTS DU DISPOSITIF ET LES PERSONNES EN CHARGE DU RECUEIL ET DU TRAITEMENT DES SIGNALEMENTS	6
06. QUELLES SONT LES PROTECTIONS ACCORDÉES AU LANCEUR D'ALERTE, AUX FACILITATEURS ET AUX PERSONNES IMPLIQUÉES ?	6
07. INFORMATION DE LA PERSONNE CONCERNÉE PAR UNE ALERTE	8
08. TRANSMETTRE UN SIGNALEMENT	8
09. TRAITEMENT DE L'ALERTE TRANSMISE PAR LE CANAL INTERNE	10
10. CONFIDENTIALITÉ	11
11. SUIVI ET PILOTAGE	11
ANNEXE 1 : INFORMATIONS SUR LE TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL	13

Procédure de recueil et de traitement des signalements

France / Corporate

01. OBJECTIFS

Dans le cadre de la volonté constante d'*emeis* de renforcer ses engagements en matière d'éthique et d'offrir des instruments facilement accessibles à tous permettant de signaler une situation inappropriée ou non conforme à ses principes ou aux lois et réglementations applicables, ***emeis* met un Dispositif d'alerte à disposition de ses collaborateurs et de ses parties prenantes.**

Ce Dispositif complète les canaux existants et renforce la démarche Éthique d'*emeis*. **Il offre à toute personne qui souhaite effectuer un signalement, un moyen facile, confidentiel et anonyme le cas échéant.**

Le Dispositif d'alerte éthique n'est en aucun cas un dispositif d'urgence et ne se substitue pas aux dispositifs existants destinés à signaler des

événements constituant une menace immédiate pour des personnes ou des biens. L'utilisation du Dispositif d'alerte reste par ailleurs facultative.

emeis a revu le Dispositif d'alerte existant et redéfinit la procédure conformément à la Directive européenne sur la protection des Lanceurs d'alerte du 23 octobre 2019 (ci-après dénommée, la « Directive européenne »). En droit français, la loi Waserman du 21 mars 2022 transpose la Directive européenne, et le décret en date du 3 octobre 2022 en précise les modalités d'application.

Enfin, *emeis* met tout en œuvre pour garantir la sécurité et la confidentialité des données communiquées dont celles à caractère personnel qui peuvent être collectées dans le but de recueillir et de traiter une alerte.

La présente procédure s'applique à *emeis* S.A. et à toutes ses filiales détenues sur le territoire français. Ainsi les règles décrites dans ce document sont établies au regard du droit français.

Procédure de recueil et de traitement des signalements

France / Corporate

02. CHAMP D'APPLICATION

Le Dispositif mis en place au sein de emeis couvre les alertes relatives aux manquements et atteintes suivants :

Manquements relatifs à la violation du Code Anticorruption (article 17 de la loi dite « Loi Sapin II »)

- ▶ L'existence de conduites ou de situations contraires au Code de conduite anticorruption du Groupe, dans la mesure où celles-ci sont susceptibles de caractériser des faits de corruption ou de trafic d'influence.

Autres manquements (article 6 de la loi dite « Loi Sapin II »)

- ▶ 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.

Risques d'atteintes graves dans le cadre du devoir de vigilance du Groupe (article 1 de la loi dite de « devoir de vigilance » du 27 mars 2017)

- ▶ L'existence ou la réalisation de risques d'atteintes graves envers les droits humains et les libertés fondamentales (dont discrimination, harcèlement moral et sexuel), la santé et la sécurité des personnes ainsi que l'environnement, résultant des activités du Groupe ou de celles de ses sous-traitants ou fournisseurs avec lesquels est entretenue une relation commerciale établie, lorsque ces activités sont rattachées à cette relation.

Autres manquements au Code Éthique et RSE du Groupe.

Procédure de recueil et de traitement des signalements

France / Corporate

03. QUI PEUT ÉMETTRE UN SIGNALEMENT ?

Par voie interne



- les collaborateurs du Groupe ;
- les anciens collaborateurs, dès lors que les informations objet du signalement ont été obtenues dans le cadre de cette relation ;
- les candidats à l'embauche, dès lors que les informations objet du signalement ont été obtenues dans le cadre de cette relation ;
- les actionnaires, les associés et les titulaires de droits de vote au sein de l'assemblée générale ;
- les membres de l'organe d'administration, de direction et de surveillance ;
- les collaborateurs occasionnels.

Par voie externe



- les collaborateurs extérieurs ;
- les co-contractants ainsi que les sous-traitants (fournisseurs, prestataires, partenaires,...) ou les membres du personnel et de l'organe d'administration, de direction ou de surveillance de ces cocontractants et sous-traitants.

04. QUELS TYPES D'ACTES OU DE COMPORTEMENTS PEUT-ON SIGNALER ?

Tout manquement à nos principes éthiques, ainsi que toutes autres violations des lois et réglementations et tout incident entrant notamment, mais pas seulement, dans les domaines suivants :

- **Corruption, trafic d'influence et conflit d'intérêts**
- **Discrimination, harcèlement, santé et sécurité au travail**
- **Fraudes, détournements et vols**
- **Pratiques anticoncurrentielles**
- **Droits et protection des personnes**
- **Protection de l'environnement**
- **Non-respect des lois, des règlements ou de l'intérêt général**

Les faits, informations et documents relevant de la prise en charge des patients ou résidents ne sont pas traités par le présent Dispositif et font l'objet de procédures spécifiques au sein d'emeis via une plateforme d'écoute www.emeis.com/plateforme-ecoute et/ou un dispositif de médiation <https://www.emeis.fr/dispositif-mediation>

Procédure de recueil et de traitement des signalements

France / Corporate

05. LES RÉFÉRENTS DU DISPOSITIF ET LES PERSONNES EN CHARGE DU RECUEIL ET DU TRAITEMENT DES SIGNALEMENTS

La fonction Conformité France et la fonction Conformité Corporate sont en charge du recueil et du traitement des signalements sur leur périmètre respectif et font office de Référent Principal de l'Alerte (RPA).

Le RPA peut solliciter d'autres fonctions (Ressources Humaines, Juridique, Finance, IT, ...), ou des tiers externes du fait de leur compétence et leur impartialité à mener les investigations, dans le cadre du traitement effectif de l'alerte.

Toutes les personnes chargées de la réception et du traitement d'un signalement sont tenues de respecter une obligation de confidentialité.

06. QUELLES SONT LES PROTECTIONS ACCORDÉES AUX LANCEURS D'ALERTE, AUX FACILITATEURS ET AUX PERSONNES IMPLIQUÉES ?

Les lois nationales sur la protection des Lanceurs d'alerte (loi Wasserman) et la Directive européenne protègent les Lanceurs d'alerte contre les mesures de représailles et les sanctions.

Néanmoins, **l'auteur d'un signalement doit répondre aux conditions cumulatives suivantes pour bénéficier du statut de Lanceur d'alerte :**

- ▶ **être une personne physique** et non une personne morale (comme par exemple une entreprise, une association ou un syndicat) ;
- ▶ **agir sans contrepartie financière directe**, c'est-à-dire ne pas prétendre à être rémunéré pour le signalement effectué ;
- ▶ **être de bonne foi**, c'est-à-dire ne pas agir de façon malveillante ou par vengeance en signalant des informations qu'il sait mensongères ou erronées ;
- ▶ **avoir connaissance des faits** soit dans le contexte professionnel (le Lanceur d'alerte peut signaler des faits dont il a eu personnellement connaissance ou qui lui ont été rapportés), soit hors du contexte professionnel (le Lanceur d'alerte doit avoir eu personnellement connaissance des faits qu'il signale) ; **et**
- ▶ **être identifiable** : la plateforme de signalement est soumise à l'identification du Lanceur d'alerte. Par exception, l'anonymat est admis si la gravité des faits signalés est établie et si les faits sont suffisamment détaillés. Le Lanceur d'alerte ne pourra bénéficier des mesures de protection (voir ci-après) qu'une fois l'anonymat levé.

Procédure de recueil et de traitement des signalements

France / Corporate

Protection de l'identité du Lanceur d'alerte qui ne sera pas divulguée

Le Dispositif garantit une stricte confidentialité de l'identité du Lanceur d'alerte, des personnes concernées et des informations recueillies, à toutes les étapes du traitement de l'alerte. Les éléments de nature à identifier le Lanceur d'alerte :

- ▶ **ne peuvent jamais être divulgués à la personne concernée par l'alerte**, même si elle exerce son droit d'accès, au titre de la loi sur la protection des données ;
- ▶ **peuvent toujours être divulgués à une autorité judiciaire en cas de demande de sa part ;**
- ▶ **peuvent être divulgués**, en dehors de l'autorité judiciaire, à quiconque uniquement après avoir recueilli le consentement préalable du Lanceur d'alerte.

Protection contre des représailles éventuelles

Sous réserve d'émettre une alerte dans le respect des dispositions prévues dans le présent document, **le Lanceur d'alerte ne peut pas faire l'objet de mesures de représailles, ni de menaces ou de tentatives de recourir à ces mesures et ce, même si les faits s'avèrent par la suite inexacts ou ne donnent lieu à aucune suite.**

Protection pénale et civile (irresponsabilité pénale et civile)

La responsabilité pénale du Lanceur d'alerte ne pourra pas être engagée dès lors que le signalement est nécessaire et proportionné à la sauvegarde des intérêts en cause.

La responsabilité civile du Lanceur d'alerte ne pourra pas non plus être engagée en cas de dommages causés par le signalement s'il avait un motif raisonnable de croire à la sauvegarde des intérêts en cause.

Autres parties prenantes

Cette protection s'applique également aux :

- ▶ **facilitateurs**, entendus comme toute personne physique ou toute personne morale de droit privé à but non lucratif (syndicats et associations) qui aide un Lanceur d'alerte à effectuer un signalement dans le respect de la loi,
- ▶ **personnes physiques en lien avec le Lanceur d'alerte** (collègues et proches),
- ▶ **entités juridiques contrôlées par le Lanceur d'alerte**, pour lesquelles il travaille ou avec lesquelles il est en lien dans un contexte professionnel (par exemple un tiers fournisseur ou sous-traitant dont le Lanceur d'alerte serait dirigeant ou salarié).

Si les conditions précitées ne sont pas satisfaites, l'auteur du signalement ne bénéficie pas du statut protecteur de Lanceur d'alerte. Cependant, **même en l'absence du statut de Lanceur d'alerte, un signalement effectué de bonne foi ne donne en aucun cas lieu à des mesures répressives.**

Le Lanceur d'alerte doit agir de bonne foi, ne pas porter délibérément de fausses accusations ou avoir pour seule intention de nuire et d'en retirer un avantage personnel. Toute utilisation abusive ou de mauvaise foi du Dispositif d'alerte expose son auteur à des sanctions disciplinaires s'il s'agit d'un collaborateur salarié, ainsi qu'éventuellement à des poursuites judiciaires.

Procédure de recueil et de traitement des signalements

France / Corporate

07. INFORMATION DE LA PERSONNE CONCERNÉE PAR UNE ALERTE

Le présent Dispositif de traitement d'alertes professionnelles nécessite la mise en œuvre d'un traitement de données relatives à des personnes physiques identifiées ou identifiables. Or, toute personne concernée par un signalement qualifié de recevable qui devient une alerte (en tant que témoin, victime ou auteur présumé des faits par exemple) doit être informée du traitement de ses données dans le cadre de cette finalité en application de la réglementation applicable sur la protection des données personnelles (RGPD et LIL), ce dans un objectif de transparence et afin notamment qu'elle puisse exercer ses droits d'accès, d'opposition, de rectification ou de suppression de données (voir Annexe 1).

Néanmoins, cette information peut être différée lorsqu'il paraît nécessaire d'adopter des mesures conservatoires afin de prévenir le risque de destruction de preuves.

Pour des raisons de confidentialité et de respect de la législation en matière de protection des données, **la personne concernée par une alerte ne peut en aucun cas obtenir de la part d'emeis**, sur le fondement de son droit d'accès, **des informations concernant l'identité du Lanceur d'alerte**, ou de toute autre personne impliquée dans l'enquête.

La personne concernée par une alerte **verra son identité traitée de manière strictement confidentielle**. Les éléments de nature à l'identifier ne peuvent être divulgués qu'une fois établi le caractère fondé de l'alerte (sauf s'il s'agit de les communiquer à l'autorité judiciaire).

08. TRANSMETTRE UN SIGNALEMENT

8.1 Canaux d'alertes

Lorsqu'il a obtenu des informations dans le cadre d'activités professionnelles et portant sur des faits qui se sont produits ou sont très susceptibles de se produire dans l'entité concernée, le Lanceur d'alerte peut procéder de manière alternative ou cumulative à un signalement interne ou externe :

Par voie interne →

Conformément à la présente procédure de recueil et de traitement des signalements (voir 8.2 et 8.3 ci-après).

Par voie externe ←

Conformément aux lois en vigueur, le Lanceur d'alerte peut également, soit après avoir effectué un signalement par voie interne, soit directement, soumettre son signalement :

- aux autorités externes compétentes dont la liste figure en annexe du décret N°2022-1284 du 3 octobre 2022 ;
- au Défenseur des droits, qui l'oriente vers la ou les autorités les mieux à même d'en connaître ;
- à l'autorité judiciaire ;
- à une institution, à un organe ou à un organisme de l'Union européenne compétent pour recueillir des informations sur des violations relevant du champ d'application de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 précitée.

Procédure de recueil et de traitement des signalements

France / Corporate

8.2 Alerter en interne

En pratique, toute alerte peut être adressée par le collaborateur à sa hiérarchie (directe ou indirecte, sauf si celle-ci est impliquée) ou par l'intermédiaire de la plateforme d'alerte décrite dans le présent Dispositif.



Par la voie hiérarchique



Par la plateforme de Signalement

Si le supérieur hiérarchique est sollicité par un collaborateur, il a pour rôle de l'orienter et le conseiller et l'inciter à utiliser le Dispositif d'alerte afin de s'adresser au RPA.

emeis encourage tous les Lanceurs d'alerte à utiliser la Plateforme d'alerte présentée à la section 8.3, notamment pour les raisons suivantes :

- ▶ **Le maintien de la confidentialité et de la sécurité des communications**
- ▶ **L'efficacité, la traçabilité et la continuité de la gestion des alertes**
- ▶ **La transparence vis-à-vis du respect des règles décrites dans ce Chapitre**
- ▶ **La protection du Lanceur d'alerte**

Si le signalement est émis en dehors de la plateforme d'alerte, celui-ci pourra être intégré par le destinataire de l'alerte dans la plateforme d'alerte, après information préalable du Lanceur d'alerte et dans le respect de son anonymat s'il en a fait la demande.

8.3 Alerter en interne par l'intermédiaire de la plateforme d'alerte

Les alertes sont transmises par le biais de la plateforme disponible à l'adresse suivante :

> **emeis.signalement.net**

Ou

> ou en utilisant la ligne téléphonique suivante pour la France : **01 86 47 77 67** et en tapant le code **1989**

L'auteur du signalement est invité à suivre les étapes suivantes :

- 1. choisir une catégorie d'alerte**
- 2. renseigner ses coordonnées ou rester anonyme**
- 3. décrire les faits de façon précise et objective**
- 4. Joindre, le cas échéant, des documents**
- 5. relire et transmettre le signalement**

Lors de l'utilisation de la plateforme d'alerte, l'auteur du signalement sera invité à classer son signalement dans l'une des catégories mentionnées en section 4. Cette catégorisation pourra être modifiée après analyse par le RPA.

Il est important de partager autant d'informations que possible (preuves, documents, etc.) lors d'un signalement pour permettre au RPA d'analyser, de traiter, et d'investiguer de la manière la plus efficace possible.

Procédure de recueil et de traitement des signalements

France / Corporate

Les investigations peuvent être rendues plus difficiles, notamment si le RPA ne peut pas recueillir d'informations complémentaires auprès du Lanceur d'alerte anonyme. L'anonymat peut également rendre plus difficile la crédibilité des allégations et l'effectivité de la protection accordée au Lanceur d'alerte. Dans tous les cas, le Lanceur d'alerte qui souhaite rester anonyme est invité à donner au RPA les moyens d'échanger avec lui afin de faciliter l'investigation des faits à l'origine du signalement.

Une fois le signalement rédigé et transmis en ligne :

- ▶ **la plateforme émet automatiquement pour l'auteur du signalement un code confidentiel sécurisé** constituant son identifiant personnel, garantissant la confidentialité et la protection des données transmises. Ce code sera demandé pour toute nouvelle connexion au signalement effectué et ainsi pouvoir en consulter le suivi, y apporter des modifications éventuelles ou encore répondre et échanger avec les personnes en charge du traitement
- ▶ dans le même temps, **un message de notification automatique est transmis par la plateforme au RPA**

09. TRAITEMENT DE L'ALERTE TRANSMISE PAR LE CANAL INTERNE

9.1 Accusé de réception du signalement et information du Lanceur d'alertes

A compter du dépôt du signalement, le RPA accuse réception par écrit auprès de l'auteur du signalement dans un délai maximum de 7 jours. Ce message précise notamment :

- ▶ **la bonne réception du signalement**
- ▶ **le délai raisonnable et prévisible nécessaire à l'examen de sa recevabilité (habituellement de 30 jours, au cas de circonstances exceptionnelles)**

9.2 Analyse de la recevabilité du signalement

Le RPA procède à un examen indépendant et objectif de la recevabilité du signalement afin de savoir si ce dernier entre dans le champ d'application du Dispositif.

Il pourra être demandé à l'auteur du signalement de fournir tout complément d'information nécessaire pour procéder à cette analyse. En absence de réponse de la part de l'auteur du signalement, ou si les éléments d'informations complémentaires communiqués demeurent non satisfaisants, le signalement sera jugé non recevable.

Les signalements jugés **non recevables sont clôturés pour irrecevabilité.**

Les signalements jugés **recevables sont qualifiés d'alerte et font l'objet d'une instruction** (voir 9.3 ci-après).

L'auteur de l'alerte est informé dans un délai de 30 jours à compter de la date d'accusé de réception **de la recevabilité ou de l'irrecevabilité** de son signalement.

Procédure de recueil et de traitement des signalements

France / Corporate

9.3 Instruction de l'alerte

Dans le cadre du traitement de l'alerte, des investigations internes ou externes seront réalisées afin de déterminer si les faits sont avérés.

En fonction de l'alerte, le RPA peut :

- ▶ **traiter l'alerte directement** en se faisant accompagner par des personnes compétentes de l'Entité *emeis* ou par un externe
- ▶ **déléguer le traitement** de l'alerte à une fonction compétente

Le délai nécessaire au traitement d'une alerte peut varier en fonction de sa complexité et des démarches de recherches et de vérifications devant être engagées dans ce cadre.

9.4 Clôture de l'alerte

Le RPA informe le Lanceur d'alerte et les personnes concernées par l'alerte du résultat du traitement et des conclusions, et le cas échéant, des mesures prises.

L'information du Lanceur d'alerte doit intervenir dans un délai de trois (3) mois à compter de l'accusé de réception de son signalement.

10. CONFIDENTIALITÉ

Le RPA et les personnes amenées à prendre part au traitement de l'alerte prennent **toutes les mesures appropriées pour se conformer aux lois applicables sur la protection des données**, d'une part, **et le secret médical**, d'autre part, et **préserver la confidentialité des informations**, que ce soit pendant leur collecte, traitement et stockage / archivage.

Toutes les alertes sont traitées dans la plus stricte confidentialité et ne sont pas divulguées en dehors des destinataires autorisés à recevoir ou à enquêter sur les alertes.

Les destinataires de l'alerte sont soumis à **une obligation de confidentialité renforcée**. Les éléments de nature à identifier le Lanceur d'alerte **ne peuvent être divulgués qu'avec le consentement de celui-ci** (sauf s'il s'agit de les communiquer à une autorité judiciaire).

Les éléments de nature à identifier la personne mise en cause par un signalement ne peuvent être divulgués qu'une fois établi le caractère fondé de l'alerte (sauf s'il s'agit de les communiquer à une autorité judiciaire).

Procédure de recueil et de traitement des signalements

France / Corporate

11. SUIVI ET PILOTAGE

Un comité de pilotage de suivi des alertes est mis en place en France et au Corporate. Ces deux comités s'assurent notamment de la correcte mise en œuvre de la présente procédure. Ils ont accès à des états de suivi préparés par les RPA. Ces états recensent les alertes reçues et l'avancée de leur traitement.

La présente procédure pourra faire l'objet de modifications en tant que de besoin par la fonction Conformité Groupe. Ces modifications peuvent être effectuées à tout moment pour rendre compte notamment d'évolutions réglementaires, ou intégrer de nouvelles spécificités identifiées.

Version initiale : 2018

Version actuelle : 31 juillet 2023

Procédure de recueil et de traitement des signalements

France / Corporate

ANNEXE 1 : INFORMATIONS SUR LE TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL

Responsable du traitement

Les données à caractère personnel recueillies font l'objet d'un traitement dont le responsable de traitement est *emeis* S.A., sis 12 rue Jean Jaurès, 92800 Puteaux.

Finalités et bases légales du traitement

Le Dispositif d'alerte est destiné à recueillir et traiter de manière appropriée des signalements relatifs à l'existence de conduites ou de situations contraires à la législation, la réglementation ou un code de conduite éthique et RSE applicables.

Obligation légale du Groupe

Ce Dispositif d'alerte est mis en place par le Groupe aux fins de se conformer aux dispositions de la Loi Sapin II pour permettre aux « membres du personnel et aux collaborateurs extérieurs et occasionnels » d'un organisme, de signaler :

- ▶ un crime ou délit ;
- ▶ une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France ;
- ▶ une violation grave et manifeste d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un engagement international régulièrement ratifié ;
- ▶ une violation grave et manifeste de la loi ou du règlement ;
- ▶ une menace ou préjudice grave pour l'intérêt général, dont l'émetteur de l'alerte a eu personnellement connaissance.

Ce Dispositif d'alerte est également mis en place par le Groupe aux fins de se conformer aux dispositions de la Loi « devoir de vigilance » et permettre le recueil des signalements relatifs à l'existence ou à la réalisation des risques d'atteintes graves envers les droits humains et les libertés fondamentales, la santé et la sécurité des personnes ainsi que l'environnement, résultant des activités de la société et de celles des sociétés qu'elle contrôle au sens du II de l'article L. 233-16, directement ou indirectement, ainsi que des activités des sous-traitants ou fournisseurs avec lesquels est entretenue une relation commerciale établie, lorsque ces activités sont attachées à cette relation.

Intérêt légitime poursuivi par le Groupe ou par le destinataire des données

Ce Dispositif d'alerte est enfin mis en place par le Groupe sur une base volontaire, en dehors d'une obligation légale spécifique, pour permettre à *emeis* et/ou l'une quelconque de ses filiales d'être informée(s) et en mesure d'agir promptement et de manière appropriée en cas de violation ou de suspicion de violation de toute législation ou réglementation ou code de conduite applicable.

Procédure de recueil et de traitement des signalements

France / Corporate

Données à caractère personnel concernées

Les données susceptibles d'être traitées dans le cadre de la procédure d'alerte emeis sont limitées aux informations suivantes :

- › identité, fonction et coordonnées de l'auteur du signalement
- › identité, fonction et coordonnées des personnes faisant l'objet d'une alerte
- › identité, fonction et coordonnées des personnes intervenant dans le recueil et/ou dans le traitement de l'alerte
- › faits signalés
- › éléments recueillis dans le cadre de la vérification des faits signalés
- › compte-rendu des opérations de vérification
- › suites données à l'alerte
- › données révélant l'état de santé, l'origine raciale ou ethnique, la religion, la vie et l'orientation sexuelle, les opinions politiques ou l'appartenance syndicale : si traitement de ces données nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice
- › informations relatives aux infractions ou condamnations dont une personne a fait l'objet : si traitement autorisé par le droit national ou pour permettre au Groupe de préparer, d'exercer et de suivre une action en justice en tant que victime, mise en cause, ou pour le compte de ceux-ci

Destinataires des données

Les Données à caractère personnel traitées dans le cadre du Dispositif d'alerte ne sont destinées qu'aux personnes habilitées, à savoir :

- › En interne : personnes spécialement chargées de la gestion des alertes au sein du Groupe ; RPA ; comité de pilotage de suivi des alertes (en France et au niveau Corporate)
- › En externe : autorité judiciaire ; sous-traitant gérant la plateforme de gestion des alertes professionnelles

Transfert en dehors de l'Union européenne (UE)

Le Groupe fait appel à un sous-traitant basé en France pour la gestion de la plateforme de gestion des alertes professionnelles, amené lui-même à sous-traiter partiellement cette prestation à un tiers situé hors UE, dont le personnel se trouve physiquement hors UE.

Afin d'encadrer ce transfert de données, et conformément au RGPD, des clauses contractuelles types ont été conclues et permettent de garantir un niveau de protection de vos données personnelles au moins équivalent à celui assuré au sein des pays de l'UE.

Procédure de recueil et de traitement des signalements

France / Corporate

Durées de conservation des données à caractère personnel

Les Données à caractère personnel collectées et traitées dans le cadre du Dispositif d'alerte sont conservées uniquement pendant le temps strictement nécessaire aux finalités poursuivies, comme décrit ci-dessous :

- ▶ Si le signalement est jugé irrecevable (non constitutif d'une alerte), les données sont sans délai détruites ou anonymisées.
- ▶ Si le signalement est jugé recevable (constitutif d'une alerte) mais que l'alerte est classée sans suite après instruction, les données sont conservées deux (2) mois à compter de la clôture des opérations de vérification, puis supprimées ou anonymisées.
- ▶ Si les faits issus de l'alerte sont établis mais ne donnent pas lieu à une procédure disciplinaire ou judiciaire, les données sont conservées pendant six (6) ans puis supprimées (ou anonymisées).
- ▶ Si l'alerte est suivie d'une procédure disciplinaire ou judiciaire à l'encontre de la personne mise en cause ou de l'auteur d'une alerte abusive, les données sont conservées jusqu'au terme de la procédure et jusqu'à la prescription des recours à l'encontre de la décision.

Exercice des droits relatifs au traitement des données personnelles

En application des articles 15 et suivants du RGPD, toute Personne concernée dont les données à caractère personnel sont collectées et traitées via le Dispositif d'alerte dispose du droit de demander à *emeis* ou à l'une quelconque de ses filiales (lorsque le signalement est émis par l'un des membres de son personnel ou l'un de ses collaborateurs extérieurs ou bien lorsque les faits signalés concerne ladite filiale), l'accès à ses données à caractère personnel, leur rectification et, si les conditions sont remplies, l'effacement de celles-ci, une limitation de leur traitement, le droit de s'opposer au dit traitement et le droit à la portabilité de ses données à caractère personnel.

Enfin, en application de la Loi Informatique et Libertés, toute personne concernée dispose du droit de définir des directives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès.

Toute personne concernée peut exercer ses droits en écrivant à l'adresse électronique suivante : dpo@emeis.com, en indiquant sa demande précisément et en y joignant un justificatif d'identité. Cette demande peut également être formulée par voie postale à l'adresse suivante :

emeis - Délégué à la Protection des Données, 12 rue Jean Jaurès, CS 10032, 92 813 Puteaux Cedex.

Toute personne a également la possibilité d'introduire une réclamation auprès de la Commission Nationale de l'Informatique et des Libertés (« Cnil ») à l'adresse suivante :

3 place de Fontenoy - TSA 80715 - 75334 Paris Cedex 07.