

Procédure de recueil et de traitement des signalements

Belgique



Procédure de recueil et de traitement des signalements

Belgique

01.	OBJECTIFS	3
02.	CHAMP D'APPLICATION	3
03.	QUI PEUT ÉMETTRE UN SIGNALEMENT ?.....	6
04.	QUELS TYPES D'ACTES OU DE COMPORTEMENTS PEUT-ON SIGNALER ?.....	6
05.	LES RÉFÉRENTS DU DISPOSITIF ET LES PERSONNES EN CHARGE DU RECUEIL ET DU TRAITEMENT DES SIGNALEMENTS	8
06.	QUELLES SONT LES PROTECTIONS ACCORDÉES AU LANCEUR D'ALERTE, AUX FACILITATEURS ET AUX PERSONNES IMPLIQUÉES ?	8
07.	INFORMATION DE LA PERSONNE CONCERNÉE PAR UNE ALERTE.....	11
08.	TRANSMETTRE UN SIGNALEMENT	12
09.	TRAITEMENT DE L'ALERTE TRANSMISE PAR LE CANAL INTERNE	13
10.	CONFIDENTIALITÉ.....	14
11.	SUIVI ET PILOTAGE	15
	ANNEXE 1 : INFORMATIONS SUR LE TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL	16

Procédure de recueil et de traitement des signalements

Belgique

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

Belgique

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.

- ▶ Le Dispositif mis en place au sein de *emeis* Belgique couvre les alertes relatives aux manquements et atteintes suivants :
- ▶ Les infractions qui tombent dans le champ d'application de la Directive Européenne et de la loi Belge :
 - ▶ marchés publics;
 - ▶ services, produits et marchés financiers et prévention du blanchiment de capitaux et du financement du terrorisme;
 - ▶ sécurité et conformité des produits;
 - ▶ sécurité des transports;
 - ▶ protection de l'environnement;
 - ▶ radioprotection et sûreté nucléaire;
 - ▶ sécurité des aliments destinés à l'alimentation humaine et animale, santé et bien-être des animaux;
 - ▶ santé publique;
 - ▶ protection des consommateurs;
 - ▶ protection de la vie privée et des données à caractère personnel, et sécurité des réseaux et des systèmes d'information;
 - ▶ lutte contre la fraude fiscale;

Procédure de recueil et de traitement des signalements

Belgique

- lutte contre la fraude sociale.
- ▶ Toute violation des dispositions légales ou réglementaires ou des dispositions européennes directement applicables.
- ▶ Les violations portant atteinte aux intérêts financiers de l'Union européenne.
- ▶ Les violations relatives au marché intérieur de l'Union européenne.
- ▶ Les infractions qui ne tombent pas directement dans le champ d'application de la Directive Européenne et de la loi Belge mais qui peuvent toujours constituer une conduite illégale, contraire à l'éthique ou non légitime, suspectée ou avérée (tentative). Exemples : pratiques anticoncurrentielles, discrimination, harcèlement, corruption, fraude
- ▶ Manquements au Code de Conduite éthique et RSE du Groupe.

Procédure de recueil et de traitement des signalements

Belgique

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.
- Employés dont le contrat de travail a été résilié
- Facilitateurs (ceux qui assistent le déclarant pendant le processus de signalement et dont l'aide doit rester confidentielle)
- Tiers liés au déclarant et risquant des représailles dans un contexte professionnel (tels que collègues, membres de la famille du déclarant)
- Entités juridiques détenues ou liées à des contextes liés au travail avec les déclarants
- Déclarants transmettant des informations acquises en dehors d'un contexte professionnel, dans la mesure où il s'agit d'une violation des services financiers, des produits et des marchés ou des violations liées à la prévention du blanchiment d'argent et du financement du terrorisme
- En ce qui concerne toute organisation, qu'elle ait ou non une personnalité juridique, relevant de la compétence des entités fédérées dans la mesure où une question n'est pas réglementée par la législation des régions et communautés relevant de la compétence de l'État fédéral, sous réserve de l'application de mesures de protection plus favorables pour le déclarant

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

Procédure de recueil et de traitement des signalements

Belgique

- ▶ 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 Belgium via le service Médiation : <https://emeis.be/fr/service-mediation-emeis-belgium>.

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

La fonction Conformité Northern Europe 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 du 28 novembre 2022 relative à la protection des personnes qui signalent des violations au droit de l'Union ou au droit national constatées au sein d'une entité juridique du secteur privé) 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 :

- ▶ facilitateur : une personne physique qui aide un auteur de signalement au cours du processus de signalement et dont l'aide devrait être confidentielle.

Procédure de recueil et de traitement des signalements

Belgique

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.

Interdiction de représailles

Les personnes faisant des signalements d'infractions sont protégées contre des sanctions ou mesures en raison d'un signalement (appelées représailles). La loi énumère les différents types de représailles interdites, à savoir :

1° suspension, licenciement ou mesures similaires ; 2° dégradation ou refus de promotion ; 3° transfert de responsabilités, changement de lieu de travail, réduction de salaire, modification des horaires de travail ; 4° refus de formation ; 5° évaluation négative des performances ou référence défavorable ; 6° imposition ou application de mesures disciplinaires ; réprimande ou toute autre sanction, y compris une sanction financière ; 7° contrainte, intimidation, harcèlement ou exclusion ; 8° discrimination, traitement défavorable ou inégal ; 9° non-conversion d'un contrat de travail temporaire en contrat de travail permanent, lorsque le salarié avait une confiance légitime qu'une embauche permanente lui serait proposée ; 10° non-renouvellement ou résiliation anticipée d'un contrat de travail temporaire ; 11° préjudice, y compris préjudice à la réputation de la personne, notamment sur les médias sociaux, ou préjudice financier, y compris perte de chiffre d'affaires et perte de revenus [...]

Pour éviter les représailles, diverses mesures de protection ont été mises en place :

- ▶ Le travailleur peut déposer une plainte motivée auprès du coordinateur fédéral, qui engage ensuite une procédure de protection extrajudiciaire.
- ▶ Un déclarant n'est pas responsable de la déclaration ou de la divulgation d'informations qu'il a légalement ou illégalement obtenues ou auxquelles il avait accès, pour autant qu'il ait des motifs raisonnables de croire que la déclaration ou la divulgation était nécessaire pour mettre en lumière l'infraction.
- ▶ Le travailleur peut saisir le tribunal du travail s'il est victime de représailles, si nécessaire sous forme d'une procédure en référé. Si le travailleur estime avoir subi un préjudice, il est présumé que ce préjudice est la conséquence des représailles.
- ▶ La divulgation de secrets d'entreprise par le travailleur n'est pas considérée comme illicite si la déclaration ou la divulgation relève du champ d'application de la loi.
- ▶ L'identité du travailleur sur lequel porte la déclaration est protégée pendant l'enquête. Les règles visant à protéger l'identité du déclarant (voir ci-dessous) s'appliquent également à lui/elle.

Si la victime de représailles est un employé, la loi prévoit l'attribution d'une indemnité forfaitaire, dont le montant s'élève à 18 à 26 semaines de salaire (cette indemnité ne peut pas être cumulée avec une indemnité accordée en vertu de la CCT n° 109 pour un licenciement manifestement déraisonnable) ; s'il s'agit d'une autre personne, l'indemnité correspond aux dommages réellement subis et la victime doit en démontrer l'étendue.

Procédure de recueil et de traitement des signalements

Belgique

Un déclarant signalant une infraction dans le domaine des services financiers, des produits et des marchés peut demander une indemnisation, soit d'un montant forfaitaire équivalent à 6 mois de salaire brut, soit des dommages réellement subis. Pour ces infractions, le déclarant licencié ou dont les conditions de travail ont été modifiées peut également demander à être réintégré ou à voir ses conditions de travail respectées.

Pour bénéficier du mécanisme de protection institué par la loi, le déclarant doit remplir les conditions suivantes :

- a) avoir eu des raisons fondées de croire que les informations signalées concernant les infractions étaient exactes au moment de la déclaration et que les informations relevaient du champ d'application de la loi (par comparaison avec une personne placée dans une situation similaire et disposant de connaissances similaires) ; et
- b) avoir effectué une déclaration interne ou externe, ou une divulgation, conformément à la loi.

Le premier critère est évalué par rapport à une personne se trouvant dans une situation similaire et ayant des connaissances similaires.

Le déclarant ne perd pas le bénéfice de la protection simplement parce que la déclaration de bonne foi a été jugée incorrecte ou infondée.

Si la protection est accordée à un facilitateur, à un tiers ou à une entité juridique, ils doivent avoir des motifs raisonnables de croire que le déclarant relevait de la protection prévue par la loi.

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.

Outre l'indemnité forfaitaire (ou l'indemnisation des dommages réels), la loi prévoit d'autres sanctions :

Amendes

Les infractions aux dispositions de la loi concernant les déclarations internes et leur suivi sont sanctionnées par une peine de niveau 4 en vertu du nouvel article 133/1 du Code pénal social, soit une peine d'emprisonnement de 6 mois à 3 ans et/ou une amende pénale de 4 800 à 48 000 EUR, soit une amende administrative de 2 400 à 24 000 EUR (par employé).

Ces sanctions s'appliquent à l'employeur, à son délégué ou à son mandataire ayant commis une infraction relative aux déclarations internes ou à l'enregistrement des déclarations.

De plus, des personnes morales du secteur privé, leurs employés ainsi que toute personne physique ou morale peuvent se voir infliger une peine de prison de 6 mois à 3 ans et/ou une amende de 4 800 à 48 000 EUR si elles commettent les infractions suivantes :

- ▶ entraver ou tenter d'entraver la déclaration ;
- ▶ prendre des représailles contre les personnes ;
- ▶ engager des procédures inutiles ou vexatoires contre les personnes visées à l'article 3 ;
- ▶ ne pas respecter l'obligation de confidentialité de l'identité des déclarants

Code pénal

- ▶ Les articles 443 à 450 du Code pénal sanctionnent le déclarant lorsqu'il est établi qu'il a délibérément fourni de fausses

Procédure de recueil et de traitement des signalements

Belgique

informations dans sa déclaration ou sa divulgation.

- ▶ Responsabilité (extra)contractuelle
- ▶ Si une personne subit un préjudice en raison d'une déclaration ou d'une divulgation faite délibérément sur la base d'informations fausses (voir l'article 8.2 ci-dessus), elle a le droit à des mesures de réparation du préjudice conformément à la responsabilité contractuelle ou extracontractuelle.

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.

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), 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).

Procédure de recueil et de traitement des signalements

Belgique

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 	Par voie externe 
Conformément à la présente procédure de recueil et de traitement des signalements (voir 8.2 et 8.3 ci-après).	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 : <ul style="list-style-type: none">- aux autorités externes compétentes belges dont la liste figure dans l'Arrêté royal du 22 janvier 2023 portant désignation des autorités compétentes pour la mise en oeuvre de la loi du 28 novembre 2022 sur la protection des personnes qui signalent des violations au droit de l'Union ou au droit national constatées au sein d'une entité juridique du secteur privé;- 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..

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

Procédure de recueil et de traitement des signalements

Belgique

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

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.

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, sauf circonstances exceptionnelles)**

Procédure de recueil et de traitement des signalements

Belgique

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.

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

Belgique

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

Belgique

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

Belgique

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 Belgique 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

Belgique

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.

Toute personne concernée peut exercer ses droits en écrivant à l'adresse électronique suivante : dpo.be@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 Belgium – Délégué à la Protection des Données, Chaussée d'Alseberg 1037, 1180 Uccle.

Toute personne a également la possibilité d'introduire une réclamation auprès d'une autorité de contrôle. Pour en savoir plus, nous vous invitons à consulter vos droits sur le site de l'Autorité de protection des données belge. (<https://www.autoriteprotectiondonnees.be/>).

Rue de la Presse 35, 1000 Bruxelles