SFA GROUP
Agitateur d'eau

PROCÉDURE DISPOSITIF LANCEUR D'ALERTE

2022/FR (V20072022)

Table des matières

1. Préambule

Cette procédure présente le cadre du **Dispositif Lanceur d'alerte.**

La présente procédure a été élaborée en collaboration avec le cabinet d'avocats LERINS & BWC Conformément à la loi " Sapin 2 " du 9 décembre 2016 et suivantes.

Ce dispositif est applicable au sein du Groupe SFA.

Il a été validé par le comité d'éthique du Groupe SFA.

L'opposabilité du Code sera mise en œuvre en l'annexant au règlement intérieur dans le respect des conditions prévues à l'article L. 1321-4 du code du travail.

2. Auteur de l'alerte

Cette procédure d'alerte professionnelle s'adresse aux **personnes physiques**, ci-après indiquées, qui ont obtenu, dans le cadre de leurs activités professionnelles, des informations portant sur des faits qui se sont produits ou sont très susceptibles de se produire dans l'entité concernée, et qui souhaitent signaler ou divulguer ces faits, et notamment:

- un membre du personnel du Groupe SFA ;
- une personne dont la relation de travail au sein du Groupe SFA s'est terminée, lorsque les informations ont été obtenues dans le cadre de cette relation ;
- un actionnaire, un associé et un titulaire de droits de vote au sein de l'assemblée générale de l'entité ;
- un membre de l'organe d'administration, de direction ou de surveillance ;
- un cocontractant, son sous-traitant ou un membre de l'organe d'administration, de direction ou de surveillance de ce cocontractant ou de son sous-traitant ainsi que les membres de leur personnel ;
- un collaborateur extérieur et occasionnel, incluant, à titre non limitatif :
- un salarié mis à disposition par une entreprise tierce ;
- un intérimaire ;
- un stagiaire ou alternant ;
- un consultant ou prestataire indépendant ;
- un sous-traitant.

IDENTIFICATION DU LANCEUR D'ALERTE

Il est recommandé au lanceur d'alerte de décliner son identité (nom, prénom et coordonnées) dans son alerte afin d'assurer son identification claire et précise.

L'identification du lanceur d'alerte lui permettra donc de bénéficier de la protection du dispositif d'alerte professionnelle, ainsi qu'une meilleure gestion et un traitement plus rapide de l'alerte.

L'identité du lanceur d'alerte, ainsi que toutes les informations recueillies dans le cadre de l'alerte, seront traitées de manière strictement confidentielle.

3. Objet de l'alerte

3.1 Faits inclus dans le champ de l'alerte

1 **Un crime ou un délit**

- **Exemples de crimes** : meurtre, viol, vol avec violences ayant entraîné une infirmité permanente, etc.
- **Exemples de délits :** corruption, fraude fiscale, prise illégale d'intérêts, discrimination, harcèlement moral ou sexuel, violation du secret des correspondances, abus de bien social, abus de confiance, trafic d'influence, etc.

2 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.

3 Une menace ou un préjudice pour l'intérêt général

- Appréciation au cas par cas des situations susceptibles de menacer ou de porter atteinte à l'intérêt général, sans que soit en jeu une infraction pénale ou une violation du droit.
- **Exemples** : atteintes à la santé publique, à la sécurité publique ou l'environnement, optimisation fiscale agressive, grave erreur de gestion, ou encore dissimulation des preuves afférentes à toutes les alertes protégées.

3.2 Faits exclus du champ de l'alerte

Sont expressément exclus du périmètre de l'alerte professionnelle les faits, informations ou documents, quel que soit leur forme ou leur support, dont la révélation ou la divulgation est interdite par les dispositions relatives au :

- secret de la défense nationale ;
- secret médical ;
- secret des délibérations judiciaires ;
- secret de l'enquête ou de l'instruction judiciaire ;
- secret professionnel de l'avocat.

Le secret ne concerne pas les faits manifestement rendus publics.

4. Conditions de l'alerte

Le lanceur d'alerte doit, lorsqu'il signale ou divulgue l'un des faits précités ci-dessus, être de bonne foi et agir sans contrepartie financière directe.

Le lanceur d'alerte ne doit pas tirer un avantage, financier ou autre, du signalement

Le lanceur d'alerte ne doit pas être animé par un grief ou une animosité personnelle ou par une intention de nuire

Le lanceur d'alerte doit avoir des motifs raisonnables permettant de croire à la véracité des dysfonctionnements signalés

Il n'est pas nécessaire que le lanceur d'alerte ait eu **personnellement** connaissance des faits en cause lorsque les informations ont été obtenues dans le cadre des activités professionnelles. Le lanceur peut ainsi signaler des faits qui lui ont été rapportés.

En revanche, lorsque les informations ont été obtenues en dehors du cadre des activités professionnelles, le lanceur d'alerte doit en avoir eu personnellement connaissance. Il doit être à la source de l'information et ne pas la détenir d'une autre personne. Le signalement doit alors porter sur des éléments dont le lanceur d'alerte est en mesure d'apprécier lui-même la réalité.

Le cas échéant, le lanceur d'alerte doit fournir tout fait, document et/ou information, quel que soit sa forme ou son support de nature à étayer son signalement.

5. Protection du lanceur d'alerte

5.1 Stricte confidentialité

Le **lanceur d'alerte,** les **personnes visées par l'alerte** et **tout tiers mentionné dans le signalement**, ainsi que **l'ensemble des informations** recueillies dans le cadre du présent dispositif seront confidentielles, y compris en cas de communication à des tiers dès lors que celle-ci est nécessaire pour les seuls besoins de la vérification ou du traitement du signalement.

Les éléments de nature à identifier le lanceur d'alerte ne peuvent être divulgués qu'avec le consentement de celui-ci.

Par exception, ils peuvent toutefois être communiqués à l'autorité judiciaire, dans le cas où les personnes chargées du recueil ou du traitement des signalements sont tenues de dénoncer les faits à celle-ci. Le lanceur d'alerte en est alors informé (avec explications écrites), à moins que cette information ne risque de compromettre la procédure judiciaire.

» La personne qui fait l'objet de l'alerte ne peut en aucun cas obtenir communication des informations concernant l'identité du lanceur d'alerte.

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

» **LE FAIT DE DIVULGUER LES ÉLÉMENTS CONFIDENTIELS PRÉCITÉS EST PUNI DE DEUX ANS D'EMPRISONNEMENT ET DE 30 000 D'AMENDE**

5.2 Conditions applicables à la protection des lanceurs d'alerte

Le lanceur d'alerte bénéficie des protections prévues dans la présente procédure si :

» ayant eu connaissance des informations concernées dans le cadre de ses activités professionnelles, il adresse un signalement interne dans les conditions définies ici ;

» il adresse un signalement externe dans les conditions définies ici, après avoir adressé un signalement interne ou directement ;

» il procède à une divulgation publique, dans les conditions définies ici.

Lorsqu'un signalement ou une divulgation publique a été réalisé de manière anonyme, le lanceur d'alerte, dont l'identité est révélée par la suite, bénéficie des mêmes protections.

5.3 Irresponsabilité pénale en matière de violation d'un secret protégé par la loi

Le lanceur d'alerte, et son complice le cas échéant, bénéficie d'une immunité pénale. A ce titre, le lanceur d'alerte ne peut être condamné pénalement pour avoir communiqué une information couverte par un des secrets protégés par la loi, à condition :

» que la divulgation soit nécessaire et proportionnée à la sauvegarde des intérêts en cause ;

» que la divulgation intervienne dans le respect des conditions d'alerte définies ici ;

» que la personne à l'origine de l'alerte réponde aux critères de définition du lanceur d'alerte.

Le lanceur d'alerte, et son complice le cas échéant, n'est pas non plus pénalement responsable s'il soustrait, détourne ou recèle les documents ou tout autre support contenant les informations **dont il a eu connaissance de manière licite** et qu'il signale ou divulgue dans les conditions indiquées ci-avant.

5.4 Interdiction de toute sanction et de toute mesure discriminatoire

Aucune personne ne peut être écartée d'une procédure de recrutement ou de l'accès à un stage ou à une période de formation en entreprise, aucun salarié ne peut être sanctionné, licencié ni faire l'objet d'une mesure discriminatoire, directe ou indirecte, notamment en matière de rémunération, de mesures d'intéressement ou de distribution d'actions, de formation, de reclassement, d'affectation, de qualification, de classification, de promotion professionnelle, d'horaires de travail, d'évaluation de la performance, de mutation ou de renouvellement de contrat ni de toute autre mesure de représailles, menaces ou tentatives d'y recourir, pour avoir :

i. relaté ou témoigné, de bonne foi, de faits constitutifs d'un délit ou d'un crime dont elle a eu connaissance dans l'exercice de ses fonctions ;

ii. signalé ou divulgué des informations dans les conditions définies ici ;

iii. subi ou refusé de subir des agissements répétés de harcèlement moral ou ayant, de bonne foi, relaté ou témoigné de tels agissements ;

iv. subi ou refusé de subir des faits de harcèlement sexuel, y compris, si les propos ou comportements n'ont pas été répétés, ou ayant, de bonne foi, témoigné de faits de harcèlement sexuel ou relaté de tels faits.

Par ailleurs, ces personnes bénéficient, notamment, des protections mentionnées aux articles 5.5, 5.7 et 5.8 ci-dessous.

5.5 Irresponsabilité civile et pénale en matière de divulgation d'informations

Les personnes ayant signalé ou divulgué publiquement des informations dans les conditions ici prévues (ainsi que les facilitateurs[1] et les personnes physiques en lien avec le lanceur d'alerte[2]), ne sont pas civilement responsables des dommages causés du fait de leur signalement ou de leur divulgation publique dès lors qu'elles avaient des motifs raisonnables de croire, lorsqu'elles y ont procédé, que le signalement ou la divulgation publique de l'intégralité de ces informations était nécessaire à la sauvegarde des intérêts en cause.

Les personnes ayant signalé ou divulgué des informations dans les conditions ici prévues ne sont pas pénalement responsables.

5.6 Interdiction des mesures de représailles, menaces ou tentatives d'y recourir

Les personnes ayant signalé ou divulgué des informations dans les conditions ici prévues (ainsi que les facilitateurs et les personnes physiques en lien avec le lanceur d'alerte) ne peuvent faire l'objet de mesures de représailles, ni de menaces ou de tentatives de recours à ce type de mesures.

En cas de représailles, les personnes susvisées bénéficient de recours et il appartient à l'autre partie de prouver que sa décision était dûment justifiée.

5.7 Sanction en cas d'obstacle à la transmission d'un signalement

Toute personne qui fait obstacle, de quelque façon que ce soit, à la transmission d'un signalement est punie d'un an d'emprisonnement et de 15 000 euros d'amende, ainsi que d'une peine complémentaire d'affichage ou de diffusion de la décision.

[1] *Loi n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte, art.2 : les facilitateurs correspondent, notamment, à toute personne physique qui aide un lanceur d'alerte à effectuer un signalement ou une divulgation dans les conditions définies ici.*

[2] *Loi n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte, art.2 : les personnes physiques en lien avec un lanceur d'alerte, sont celles qui risquent de faire l'objet de mesures de représailles, menaces ou tentatives d'y recourir dans le cadre de leurs activités professionnelles de la part de leur employeur, de leur client ou du destinataire de leurs services*

5.8 Action abusive ou dilatoire

Lors d'une procédure dirigée contre un lanceur d'alerte en raison des informations signalées ou divulguées, si la constitution de partie civile est considérée comme abusive ou dilatoire, l'amende civile susceptible d'être prononcée contre la partie civile est portée de 15 000 à 60 000 euros. Une peine complémentaire d'affichage ou de diffusion de la décision peut également être prononcée et est à la charge de la personne condamnée.

Des dommages et intérêts peuvent également être accordés au lanceur d'alerte victime de la procédure dilatoire ou abusive.

6. Procédures à suivre pour lancer l'alerte

Le signalement d'une alerte peut être réalisé, **au choix de son auteur**, selon l'une des procédures suivantes :

VOIE INTERNE

Le signalement par la voie interne doit notamment être réalisé lorsque le lanceur d'alerte estime qu'il est possible de remédier efficacement à la violation par cette voie et qu'il ne s'expose pas à un risque de représailles.
Le signalement peut être porté à la connaissance :
- du supérieur hiérarchique, direct ou indirect ;
- de l'employeur ;
- du Comité d'éthique du Groupe SFA.

VOIE EXTERNE

Le lanceur d'alerte adresse un signalement externe, soit après avoir effectué un signalement interne, soit directement à :
- l'autorité compétente ;
- au défenseur des droits, qui l'oriente vers la ou les autorités les mieux à même d'en connaitre ;
- à l'autorité judiciaire ;
- à une institution, un organe ou un organisme de l'UE.

DIVULGATION PUBLIQUE

Le lanceur d'alerte peut procéder à une divulgation publique :
- après avoir effectué un signalement externe, précédé ou non d'un signalement interne, sans qu'aucune mesure appropriée ait été prise en réponse à ce signalement à l'expiration du délai du retour d'informations
- en cas de danger grave et imminent ou, pour les informations obtenues dans le cadre de ses activités professionnelles, en cas de danger imminent ou manifeste pour l'intérêt général
- ou lorsque la saisine de l'une des autorités compétentes ferait encourir à son auteur un risque de représailles ou qu'elle ne permettrait pas de remédier efficacement à l'objet de la divulgation.

7. Destinataires de l'alerte interne

Le signalement d'une alerte par la voie interne est porté, **au choix de son auteur**, à la connaissance de son responsable, son directeur ou son représentant RH, du représentant local en matière de RSE ou du comité d'éthique du Groupe SFA ou du référent obligatoirement désigné par celui-ci (interne ou externe).

Ainsi, l'auteur de l'alerte choisit de s'adresser à l'une ou l'autre de ces personnes / entités.

Quel que soit le destinataire de l'alerte, celui-ci la transmet au Comité d'éthique chargé d'instruire ou de faire instruire l'alerte.

Le Groupe SFA a désigné comme référent susceptible de recevoir les alertes professionnelles : le prestataire **SpeakUp** de People Intouch B.V:

Web SpeakUp : https://sfagroup.speakup.report/sfagroup
App SpeakUp : Download « SpeakUp by People Intouch »

L'outil SpeakUp et son utilisation sont présentés en annexe de la présente procédure : l'outil de signalement SpeakUp, Guide à l'intention des employés».

Les membres du Comité éthique, chargées du traitement des alertes professionnelles doivent disposer de la compétence nécessaire au traitement de ces alertes (formation spécifique requise).

Ils sont de plus astreints à une obligation renforcée de confidentialité contractuellement définie.

8. Modalités d'envoi de l'alerte interne

Il est possible de signaler l'existence et/ou la survenance d'un des faits limitativement énumérés aux présentes, par : fait de corruption ou de trafic d'influence, doit le signaler :

» par Courriel :

o à l'adresse électronique du destinataire choisi : son responsable, son directeur ou son représentant RH ou de son référent RSE

o à l'adresse électronique dédiée du comité d'éthique du Groupe SFA : Ethics@sfagroup.com ;

ou

» en utilisant l'outil de signalement SpeakUp

Web SpeakUp : https://sfagroup.speakup.report/sfagroup
App SpeakUp : Download « SpeakUp by People Intouch »

N.B Tout destinataire d'une alerte la transmet au comité d'éthique du Groupe SFA par mail ou via SpeakUp.

9. Suivi et traitement de l'alerte interne

9.1 Accusé de réception

Suite à la réception de l'alerte, le lanceur d'alerte recevra les informations suivantes:

» un accusé de réception de l'alerte, dans un délai de 7 jours à compter de sa réception, par courriel à son adresse électronique professionnelle ou via l'outil de signalement SpeakUp.

» le délai raisonnable et prévisible nécessaire à l'examen de la recevabilité de son alerte ;

» les modalités suivant lesquelles il sera informé des suites données à son alerte.

Le retour d'information ne peut en aucun cas excéder **3 mois** à compter de l'accusé de réception du signalement.

9.2 Recevabilité de l'alerte

Le Comité d'éthique du Groupe SFA vérifie, dans un délai raisonnable, la recevabilité de l'alerte et notamment si :

- la personne à l'origine de l'alerte répond à la définition du lanceur d'alerte ;
- les faits signalés entrent dans l'objet de l'alerte professionnelle et se rapportent à l'activité du Groupe SFA ;
- l'alerte a été émise conformément aux règles légales propres à ce dispositif.

Pour effectuer ces vérifications, il peut être procédé à des :

- auditions de tout personnel, agent ou collaborateur extérieur ou occasionnel du Groupe SFA ;
- investigations dans le système d'information du Groupe SFA ;
- analyses de tout document communiqué par le lanceur d'alerte.

Le Groupe SFA peut décider de recourir à un prestataire externe soumis au secret professionnel pour effectuer cette mission de vérification, notamment dans l'hypothèse où les faits se révèleraient d'une particulière gravité ou nécessiteraient de plus amples investigations.

» Les prestataires externes susceptibles d'intervenir dans le cadre du traitement d'une alerte, ainsi que les membres du Comité d'éthique du Groupe SFA, sont soumis à une clause de confidentialité renforcée[3].

9.3 Demande d'informations complémentaires

Dès réception de l'alerte, il peut être demandé au lanceur d'alerte toutes précisions complémentaires, nécessaires à la gestion et au traitement de l'alerte. Un courriel lui sera alors envoyé à son adresse électronique professionnelle ou via l'outil SpeakUp

9.4 Rapport d'enquête

A l'issue de ces vérifications, les bonnes pratiques consistent à rédiger un **rapport interne d'enquête.**

[3] *Dans le cas du recours à un prestataire externe, le Groupe SFA conclut avec celui-ci un contrat définissant les caractéristiques du traitement ainsi que les différentes obligations des parties en matière de protection des données. RGPD, art. 28.*

Dès le traitement de l'alerte, le lanceur d'alerte est informé :

» de la recevabilité de son alerte et des actions appropriées mises en œuvre pour remédier aux faits dénoncés[4] ; ou

» de la clôture du dossier, soit en raison de l'irrecevabilité de l'alerte, soit en raison de l'absence de suites données à l'alerte. A cette occasion, il est possible d'orienter le lanceur d'alerte vers un autre service compétent.

10. Utilisation abusive du dispositif

L'utilisation du présent dispositif d'alerte de bonne foi par l'auteur d'une alerte, même si les faits s'avèrent par la suite inexacts ou ne donnent lieu à aucune suite, n'expose pas son auteur à une sanction disciplinaire.

L'utilisation **abusive** de l'alerte professionnelle est sanctionnée en raison des dommages importants qu'une telle alerte peut occasionner, tant pour les personnes physiques éventuellement visées que pour le Groupe SFA lui-même. L'utilisation abusive du dispositif peut exposer son auteur à des sanctions disciplinaires ainsi qu'à des poursuites judiciaires.

11. Protection des données à caractère personnel

Le présent dispositif d'alerte revêt un caractère facultatif et sa non-utilisation n'entraîne aucune conséquence à l'égard des personnes concernées.

11.1 Identification du traitement

Les éléments d'identification du traitement couverts par la présente procédure sont les suivants :

Responsable du traitement	Entité concernée par l'alerte
Objet du traitement	Gestion des alertes

[4] *Exemples : actions correctives internes, mesures disciplinaires à l'égard de la personne visée par l'alerte, saisine des juridictions compétentes, recommandations d'actions au lanceur d'alerte.*

Nature du traitement	Collecte, enregistrement, organisation, structuration, conservation, modification, extraction, consultation, utilisation, communication par transmission, diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, limitation, destruction.
Base légale du traitement	Les bases légales sont : - respect d'une obligation légale ; - intérêt légitime
Finalités du traitement	Les finalités sont le signalement et le traitement des alertes professionnelles.
Type de données à caractère personnel	Les données à caractère personnel collectées sont : - identité, fonctions et coordonnées de l'auteur de l'alerte; - identité, fonctions et coordonnées des personnes faisant l'objet d'une alerte ; - identité, fonctions et coordonnées des personnes intervenant dans le recueil ou dans le traitement de l'alerte ; - faits signalés ; - éléments recueillis dans le cadre de la vérification des faits signalés ; - compte rendu des opérations de vérification ; - suites données à l'alerte.
Catégorie de personnes concernées	Les personnes concernées sont : - auteur de l'alerte ; - personne visée par une alerte ; - personnes intervenant dans le recueil ou le traitement de l'alerte ; - le cas échéant, personnes interrogées dans le cadre des opérations de vérification.
Destinataires des données à caractère personnel	Les destinataires sont : - supérieur hiérarchique, direct ou indirect ; - le référent (le cas échéant, un prestataire externe (sous-traitant)) ; - les membres du Comité d'éthique du Groupe SFA(le cas échéant, un prestataire externe (sous-traitant)) ; - les éventuels auditeurs soumis à confidentialité dans le cadre d'opérations de cession / acquisition.

11.2 Droits des personnes concernées

Le responsable du traitement assure le respect des droits des personnes concernées dans le cadre du traitement de données à caractère personnel qu'il met en œuvre pour la gestion des alertes professionnelles.

11.2.1 Droit d'accès aux données à caractère personnel

Toute personne dont les données à caractère personnel font ou ont fait l'objet d'un traitement dans le cadre d'une alerte professionnelle (lanceur de l'alerte, victimes présumées des faits, personnes visées par l'alerte, personne mentionnée dans le signalement, témoins et personnes entendues lors de l'enquête, etc.), a le droit d'y avoir accès[5].

L'exercice de ce droit ne doit pas permettre à la personne qui l'exerce d'accéder aux données à caractère personnel relatives à d'autres personnes physiques. Cette limitation est propre aux règles relatives à la protection des données personnelles et ne fait pas obstacle à l'application, le cas échéant, des règles du droit processuel, des libertés fondamentales (et notamment du principe du contradictoire), etc.

11.2.2 Droit à la rectification des données à caractère personnel

Le droit de rectification doit s'apprécier au regard de la finalité du traitement[6].

Dans le cas des dispositifs d'alerte professionnelle, il ne doit notamment pas permettre la modification rétroactive des éléments contenus dans l'alerte ou collectées lors de son instruction.

Son exercice, lorsqu'il est admis, ne doit pas aboutir à l'impossibilité de reconstitution de la chronologie des éventuelles modifications d'éléments importants de l'enquête.

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

11.2.3 Droit à l'effacement des données à caractère personnel

La personne concernée peut demander l'effacement de ses données à caractère personnel lorsque l'un des motifs suivants s'applique :

[5] *RGPD, art. 15.*
[6] *RGPD, art. 16*

- les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;

- le cas échéant, la personne concernée s'oppose au traitement de ses données à caractère personnel lorsqu'il n'existe pas de motif légitime impérieux pour le traitement ;

- le traitement de données à caractère personnel n'est pas conforme aux dispositions de la réglementation applicable sur la protection des données à caractère personne[7].

Le droit à l'effacement des données à caractère personnel n'est pas un droit général et il ne pourra y être fait droit que si l'un des motifs précités s'applique.

11.2.4 Droit à la limitation des traitements de données à caractère personnel

La personne concernée a le droit d'obtenir du responsable de traitement la limitation du traitement lorsque l'un des éléments suivants s'applique :

- l'exactitude des données à caractère personnel est contestée par la personne concernée, pendant une durée permettant au responsable du traitement de vérifier l'exactitude des données à caractère personnel ;

- le traitement est illicite et la personne concernée s'oppose à leur effacement et exige à la place la limitation de leur utilisation ;

- le responsable du traitement n'a plus besoin des données à caractère personnel aux fins du traitement mais celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice[8].

11.2.5 Droit de s'opposer aux traitements de données à caractère personnel

Conformément à l'article 21 du RGPD, le droit d'opposition ne peut pas être exercé pour les traitements nécessaires au respect d'une obligation légale à laquelle est soumis le responsable du traitement[9].

Il ne peut donc pas être exercé à l'égard des traitements mis en place par le responsable de traitement, remplissant les conditions définies dans la présente procédure.

[7] RGPD, art. 17
[8] RGPD, art. 18
[9] RGPD, art. 21.

11.3 Modalités d'exercice des droits

Les demandes relatives à l'exercice des droits des personnes concernées s'effectuent :

» à l'adresse électronique suivante : Ethics@sfagroup.com

11.4 Conservation des données à caractère personnel

Les durées de conservation applicables aux données recueillies dans le cadre du dispositif d'alerte professionnelle sont les suivantes :

- lorsque l'alerte n'entre pas dans le champ du dispositif, les données seront immédiatement détruites ou anonymisées ;

- lorsqu'aucune suite[10] n'est donnée à une alerte rentrant dans le champ du dispositif, les données seront détruites ou archivées, après anonymisation, dans un délai de deux (2) mois à compter de la clôture des opérations de recevabilité ou de vérification ;

- lorsque l'alerte est suivie d'une procédure disciplinaire ou judiciaire à l'encontre d'une personne mise en cause ou de l'auteur d'une alerte abusive, les données seront détruites au terme de la procédure ou après la prescription des recours à l'encontre de la décision.

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

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

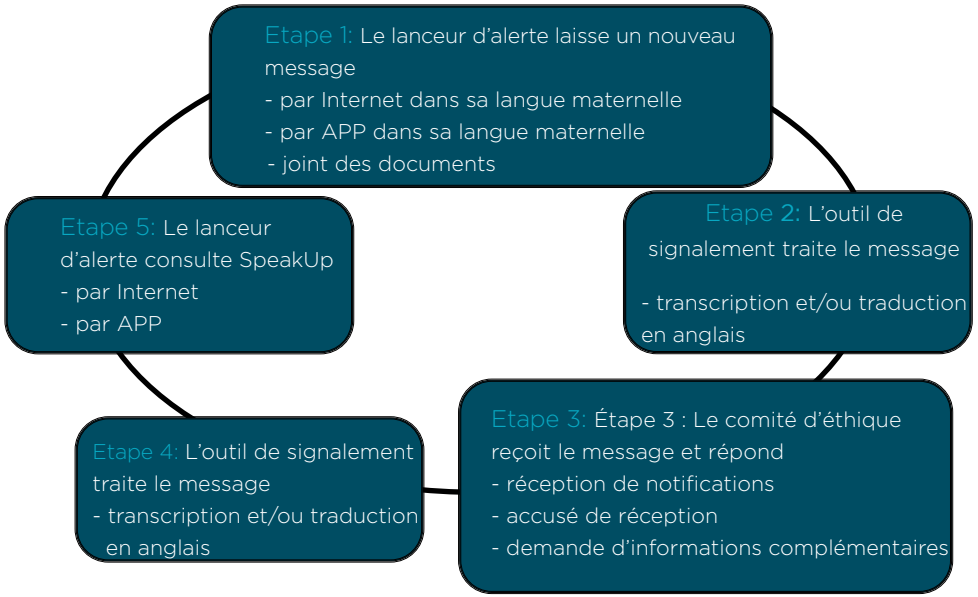
[10] *Le terme « suite » désigne toute décision prise par l'organisme pour tirer des conséquences de l'alerte. Il peut s'agir de l'adoption ou de la modification des règles internes (règlement interne, charte éthique, etc.) de l'organisme, d'une réorganisation des opérations ou des services du Groupe SFA, du prononcé d'une sanction ou de la mise en œuvre d'une action en justice.*

SFA GROUP
Agitateur d'eau

OUTIL DE SIGNALEMENT SPEAKUP, GUIDE À L'INTENTION DES EMPLOYÉS

TABLE DES MATIÈRES

1 SPEAKUP : COMMENT LAISSER UN MESSAGE



Laisser un message

Vous pouvez choisir de laisser un message par l'intermédiaire du système web ou APP de SpeakUp®.

Web SpeakUp : Veuillez vous rendre sur «https://sfagroup.speakup.report/sfagroup»
App SpeakUp : Download « SpeakUp by People Intouch »

(Nous vous conseillons d'écrire votre message au préalable ; ainsi vous êtes sûr des informations que vous vous apprêtez à communiquer et que votre message est complet et pertinent.)

Munissez-vous d'un stylo lorsque vous laissez le message. Vous recevrez un numéro de dossier personnel à six chiffres, généré de façon aléatoire. Il est très important que vous le notiez, car vous en aurez besoin pour prendre connaissance de la réponse du comité d'éthique lorsque vous re- tournerez plus tard dans le système SpeakUp®.

Si vous utilisez le système SpeakUp, vous pouvez saisir ou simplement copier/coller votre message. Vous pouvez également télécharger et joindre des documents à votre message. Lorsque vous avez terminé, appuyez sur le bouton « envoyer le message » ; un écran affichant votre numéro de dossier et votre message apparaîtra, que vous pourrez aisément imprimer.

Que se passe-t-il entre-temps ?

Dès lors que vous envoyez votre message, le système de signalement lance, si nécessaire, la traduction du message en anglais.

Une fois la transcription et la traduction effectuées, le message exact sera envoyé au comité d'éthique.

Le comité d'éthique est informé de l'alerte transmise. Il analyse les données du message et évalue la conduite à tenir pour y répondre et la traiter. Il veille au parfait anonymat du lanceur d'alerte et à sa protection. Ce dernier bénéfice d'une immunité pénale. Le comité d'éthique peut aussi décider de ne pas donner suite à l'alerte s'il l'estime irrecevable. Il peut encore décider de faire appel à un prestataire externe soumis au secret professionnel pour l'épauler dans la résolution du fait porté à connaissance.

Consultation de la réponse

Un accusé de réception vous sera adressé sous sept jours et un retour d'informations sous 90 jours sur le système SpeakUp. En général, vous pourrez consulter cette réponse de la même manière que vous avez laissé votre message, en utilisant les informations de contact susmentionnées.

Si vous remarquez qu'aucune réponse ne vous a encore été communiquée, soyez assuré que le message est en cours d'examen et qu'une réponse vous sera adressée dans les meilleurs délais. Il est conseillé de vérifier régulièrement la réception d'une réponse.

2 QUESTIONS FRÉQUEMMENT POSÉES SUR LE SYSTÈME SPEAKUP

2.1 QU'EST-CE QUE SPEAKUP ?

Il s'agit d'un outil permettant aux salariés (ou parties prenantes) de signaler de graves manquements en garantissant, s'ils le souhaitent, un anonymat complet. Vous pouvez effectuer vos signalements soit par app, soit par le biais d'un site web sécurisé, sans avoir à passer par un opérateur humain.

2.2 À QUOI L'OUTIL SPEAKUP SERT-IL ?

L'outil SpeakUp a été mis en place pour promouvoir une transparence dans les échanges professionnels et commerciaux et s'assurer que nous répondons à nos obligations légales, notamment concernant la « Directive européenne sur le

dispositif d'alerte professionnelle » protégeant le lanceur d'alerte. L'outil SpeakUp ne doit cependant pas se substituer au dialogue direct puisqu'il fait partie de notre culture d'entreprise et nous voulons absolument le préserver. Cet outil doit être utilisé en dernier recours ou parce que l'on s'aperçoit qu'il est très difficile d'en parler.

Il est également destiné à être utilisé comme un moyen de poser des questions. Cet outil peut être utilisé par des victimes ou des témoins pour se renseigner sur leurs droits de façon anonyme lorsqu'ils décident de faire un rapport.

(Notre conseil : consultez la procédure de signalement du Groupe SFA)

2.3 COMMENT FONCTIONNE SPEAKUP ?

Site web : Rendez-vous sur la page du Service web de SpeakUp (via un lien hypertexte ou en entrant l'adresse URL), sélectionnez votre pays, saisissez votre code d'accès et laissez votre message. Sous une semaine, vous pourrez retourner sur le Service web et consulter la réponse du comité d'éthique. Vous pourrez soumettre une réplique à cette réponse. Ce cycle de communication peut être répété à l'infini.

App : Accédez à l'application SpeakUp, créez un code confidentiel et scannez le QR Code du groupe SFA de SpeakUp.

2.4 QUI GÈRE SPEAKUP ?

Le service est géré par un tiers, People Intouch, une société néerlandaise indépendante. People Intouch est chargée de traiter tous les messages. Fondée en 2004, cette société est basée à Amsterdam. Le système de signalement SpeakUp® est déjà utilisé par de nombreuses entreprises renommées telles que SNCF.

2.5 LE SYSTÈME EST-IL DIFFICILE À UTILISER ?

Non, vous êtes guidé(e) à toutes les étapes.

2.6 MON IDENTITÉ PEUT-ELLE ÊTRE DÉCOUVERTE ?

Si vous laissez vos coordonnées dans votre message, SpeakUp les trans- mettra ; si vous ne communiquez pas vos coordonnées, SpeakUp et le comité d'éthique du Groupe SFA ne sauront pas qui vous êtes. De plus, l'entreprise s'est engagée à ne pas rechercher l'identité d'un appelant et ne communiquera pas l'identité de l'appelant ou d'un témoin à une personne accusée. Seules les autorités administratives compétentes (justice) pour- raient être habilitées à interroger le système en cas de délit grave.

2.7 L'ENTREPRISE PEUT-ELLE TRACER MES DONNÉES DE CONNEXION ?

Non, le système SpeakUp est géré par un tiers. Le Groupe SFA n'a aucun accès aux données de connexion. Les Adresses IP ne seront jamais trans- mises au Groupe SFA. Toutefois, il est possible que votre entreprise trace les informations utilisateur issues de votre téléphone ou ordinateur professionnel. Veuillez noter que vous pouvez également utiliser un téléphone ou un ordinateur public ou non identifiable.

2.8 QU'EN EST-IL DE L'ENREGISTREMENT DE MON MESSAGE ?

Lorsque le comité d'éthique aura accusé réception du message transcrit et/ou traduit, l'enregistrement sera immédiatement effacé par un fournisseur de logiciels externe.

2.9 LA CONFIDENTIALITÉ SERA-T-ELLE UN JOUR ROMPUE ?

Exception à ce qui précède : si le système SpeakUp reçoit un message par lequel l'appelant profère des menaces de violence ou un acte criminel, le comité d'éthique du Groupe SFA peut demander à conserver l'enregistrement en vue de le remettre aux autorités. Cependant, les données de connexion ne seront jamais transmises au comité d'éthique.

2.10 DANS QUEL DÉLAI MON MESSAGE SERA-T-IL TRANSMIS À L'ENTREPRISE ?

Votre message, une fois traduit si nécessaire, sera transmis au comité d'éthique sous un délai d'un jour ouvrable.

2.11 QUI AU SEIN DE L'ENTREPRISE REÇOIT MON MESSAGE ?

Le comité d'éthique du Groupe SFA, situé au siège de SFA à Paris. *La liste des membres du comité se trouve dans le document "Les comiés de gouvernance RSE du Groupe SFA".*

2.12 JE SOUHAITE GARDER L'ANONYMAT, MAIS J'AIMERAIS RECEVOIR UNE RÉPONSE, COMMENT PUIS-JE FAIRE ?

Le système SpeakUp vous communiquera un numéro de dossier unique. Veuillez-vous assurer de le noter avec soin. Ce numéro de dossier vous permettra d'écouter ou de lire la réponse du comité d'éthique lorsque vous retournerez dans le système.

2.13 DANS QUEL DÉLAI PUIS-JE OBTENIR UNE RÉPONSE ?

Le comité d'éthique s'efforce d'envoyer un accusé de réception sous sept jours et un retour d'informations sous 90 jours.

En l'absence de réponse au terme d'une semaine, nous vous conseillons de saisir un nouveau message dans le même dossier.

2.14 PUIS-JE LAISSER UN MESSAGE DANS MA LANGUE MATERNELLE ?

Oui, vous pouvez laisser un message dans votre langue maternelle. Des accords sont conclus avec le Groupe SFA concernant les options linguistiques pour chaque pays. Lorsque vous laissez votre message, il vous suffit de sélectionner l'une de ces langues. Les réponses seront également communiquées dans votre langue maternelle.

2.15 PUIS-JE JOINDRE DES DOCUMENTS ?

Oui, le service web de SpeakUp vous permet de joindre des documents (électroniques).

Lorsque vous laissez un message sur le système téléphonique, vous pouvez vous connecter au système web en reprenant le même numéro de dossier. Appuyez sur le bouton « si vous disposez déjà d'un numéro de dossier ». Vous pouvez déposer ici vos documents (électroniques).

Si vous souhaitez rester anonyme, assurez-vous que vos coordonnées ne figurent pas dans les pièces jointes ni dans leurs propriétés.

2.16 QUE FAIRE SI J'AI OUBLIÉ MON NUMÉRO DE DOSSIER ?

Si vous avez perdu votre numéro de dossier, nous vous demandons de laisser à nouveau votre message avec un nouveau numéro de dossier. Utilisez le nouveau numéro de dossier pour toute communication ultérieure.

2.17 JE NE SAIS PAS OU TROUVER LES INFORMAITONS POUR LAISSER UN MESSAGE. OU PUIS-JE LES TROUVER ?

Les informations pour laisser un message figurent sur la page 22.

2.18 QUE SONT LES DONNÉES À CARACTÈRE PERSONNEL ? MES DONNÉES PERSONNELLES SONT-ELLES PROTÉGÉES PAR LA LÉGISLATION SI JE LAISSE UN MESSAGE PAR L'INTERMÉDIAIRE DE SPEAKUP ?

Les données à caractère personnel sont (en bref) des informations pouvant être utilisées pour identifier (directement ou indirectement) une personne (ex. : nom, adresse, photo, numéro de téléphone), qui pourrait être vous- même ou une autre personne mentionnée dans votre message. Le traite- ment des données personnelles par le système SpeakUp est strictement réglementé (par le Règlement général sur la protection des données (RGPD)).

2.19 QUELS SONT MES DROITS SI JE LAISSE UN MESSAGE CONTENANT MES DONNÉES PERSONNELLES PAR L'INTERMÉDIAIRE DE SPEAKUP ?

Le Groupe SFA est tenu d'assurer le respect de vos droits en vertu du RGPD, notamment: le droit d'accès, le droit de rectification, le droit d'effacement/à l'oubli, le droit à la limitation du traitement, le droit à la portabilité des données, le droit d'opposition et le droit de déposer une plainte auprès de l'autorité de contrôle. Les politiques internes du Groupe SFA doivent préciser les modalités d'exercice de ces droits. Le Groupe SFA doit également aviser la personne concernée de la survenance d'une prétendue « violation des données personnelles », si celle-ci présente un risque élevé pour les droits et libertés de cette personne.

2.20 POURQUOI MON CONSENTEMENT AU TRAITEMENT DES DONNÉES PERSONNELLES N'EST-IL PAS DEMANDÉ LORSQUE JE LAISSE UN MESSAGE DANS LE SYSTÈME SPEAKUP ?

Les employés, tels que vous, n'êtes (en général) pas considérés comme étant en mesure de donner, refuser ou révoquer librement votre consentement, dans la mesure où il existe un lien de dépendance découlant de la relation employé/ employeur. Toute donnée à caractère personnel contenue dans un message qui est traitée par le système SpeakUp, est traitée au motif que cela est nécessaire pour détecter un manquement qui n'aurait pas été décelé autrement.

LA DÉMARCHE DE PRISE DE PAROLE

1. EXPRIMEZ-VOUS

Concerné par une conduite inappropriée ?

- Je crains que ce cadeau soit trop cher
- Je soupçonne une utilisation abusive des actifs de l'entreprise
- Je me sens victime de discrimination ou de harcèlement
- Je soupçonne le versement de pots-de-vin
- S'agit-il d'une fraude ?

2. À QUI PUIS-JE M'ADRESSER ?

Si possible, parlez à la personne concernée

↓

Adressez-vous à votre responsable, à votre directeur ou à votre représentant RH

↓

Contactez votre représentant local en matière de RSE

↓

Contactez le comité d'éthique du groupe SFA à l'adresse ethics@sfagroup.com

3. VOUS POUVEZ ÉGALEMENT...

(DE MANIÈRE ANONYME)

Vous rendre sur le site **https://sfagroup.speakup.report/sfagroup** pour transmettre votre réclamation

OU

Utiliser l'app. «**SpeakUp by People Intouch**» en scannant ce QR Code

Alertez avec SpeakUp

Nous comprenons qu'il n'est pas toujours facile de faire part de ses inquiétudes concernant une éventuelle faute professionnelle, mais nous vous encourageons à nous faire part de vos préoccupations et à vous exprimer ! Tout problème sera traité de manière appropriée et confidentielle.

SFA GROUP
Agitateur d'eau

SFA GROUP
Agitateur d'eau

POUR TOUTE INFORMATION SUR L'ÉTHIQUE ET LA CONFORMITÉ OU POUR RAPPORTER UN INCIDENT D'ÉTHIQUE AU GROUPE, CONTACTEZ:
ETHICS@SFAGROUP.COM

SFA
41 bis Avenue Bosquet
75007 Paris
FRANCE

2022-07-19_PROCÉDURE DISPOSITIF LANCEUR D'ALERTE