Procédure de signalement des lanceurs d'alerte de Sofidel France SAS

0	02th January 2024	*Nouvelle édition*	Fabiana Da San Martino *Responsable de la conformité*	Elena Betti *Directrice de la gestion des risques et de la conformité*
Rév	Date	Description	Rédigé	Approuvé

1. But

Le but de cette procédure est de régir les principes et les règles de gestion des signalements que Sofidel France SAS (ci-après dénommée « **la Société** ») a décidé d'adopter conformément à la politique du Groupe et à la Directive (UE) 2019/1937 (ci-après dénommée la « **Directive de *signalement des lanceurs d'alerte*** ») qui a été transposée en France par la Loi n°2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte, et le Décret subséquent n°2022-1284 du 3 octobre 2022 relatif aux procédures de recueil et de traitement des signalements émis par les lanceurs d'alerte et fixant la liste des autorités externes instituées par la loi n°2022- 401 du 21 mars 2022 (ci-après dénommée « **Loi sur les *signalements des lanceurs d'alerte*** ») qui régit la protection des personnes qui signalent des infractions aux dispositions réglementaires nationales ou de l'Union européenne affectant l'intérêt public ou l'intégrité de l'administration publique ou de l'entité privée par des lanceurs d'alerte dont ils ont eu connaissance dans le cadre de leur travail.

1.1. Références juridiques

La présente procédure est adoptée conformément aux actes réglementaires suivants :

- la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 *sur la protection des personnes qui signalent des violations du droit de l'Union* ;
- le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* ;
- la Loi n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte ;
- Décret n° 2022-1284 du 3 octobre 2022 relatif aux procédures de recueil et de traitement des signalements émis par les lanceurs d'alerte et fixant la liste des autorités externes instituées par la loi n° 2022-401 du 21 mars 2022.

Cette procédure a été élaborée en prenant en compte le référentiel relatif aux traitements de données à caractère personnel destinés à la mise en œuvre d'un dispositif d'alerte publié par la Commission nationale de l'informatique et des libertés le 6 juillet 2023.

2. Étapes du processus

2.1. Domaine d'application subjectif : les destinataires

Les destinataires de la présente procédure sont les lanceurs d'alerte potentiels. Et notamment :

- les membres du personnel ;
- les fournisseurs ;
- les actionnaires et les personnes exerçant des fonctions d'administration, de gestion, de contrôle, de surveillance ou de représentation ;
- les collaborateurs indépendants et occasionnels ;
- les cocontractants et les sous-traitants de l'entreprise ou, lorsque ces cocontractants et sous-traitants sont des personnes morales, des membres des organes d'administration, de direction ou de surveillance desdites personnes morales ou les membres de leur personnel ;
- toute personne ayant obtenu l'information dans un contexte étranger à son activité professionnelle. Néanmoins, dans ce cas, il est nécessaire que l'informateur soit personnellement au courant de l'information. Le lanceur d'alerte doit avoir fait son signalement de bonne foi, sans contrepartie financière directe.
- les clients ;

Le signalement ou la divulgation publique ne doit pas nécessairement avoir lieu dans le cadre de la relation de travail ou d'une autre relation juridique existante. Ils peuvent également être faits dans les cas suivants :

- lorsque la relation de travail est en cours ;
- lorsque la relation de travail s'est conclue, si l'information a été obtenue au cours de cette relation ;
- si la relation de travail n'a pas encore été nouée, mais a simplement fait l'objet d'une candidature, et si l'information a été obtenue dans le cadre de cette candidature ;

  dans un contexte non professionnel, à condition que le lanceur d'alerte ait eu une connaissance personnelle de l'information faisant l'objet du signalement.

2.2. Domaine d'application objectif

2.2.1. L'objet du signalement

La présente procédure couvre les signalements relatifs à :

- des violations constitutives d'un crime, d'un délit, d'une menace ou d'un préjudice pour l'intérêt général ;

- la violation ou la tentative de dissimulation de la violation d'un engagement international régulièrement ratifié ou approuvé par l'État français et la violation de tout acte unilatéral d'une organisation internationale adopté sur la base de cet engagement ;
- la violation d'une loi ou d'un règlement ;
- les violations du droit de l'Union européenne, à savoir :
    i. les infractions relevant du champ d'application des actes de l'Union européenne dans les champs suivants, dans la mesure où ils sont pertinents pour la Société : 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, santé publique, protection des consommateurs, protection de la vie privée et des données personnelles et sécurité des réseaux et des systèmes d'information ;
    ii. les actes ou omissions portant atteinte aux intérêts financiers de l'Union européenne

Ci-après figure une liste, illustrative et non exhaustive de violations portant atteinte aux intérêts financiers de l'Union européenne, telles qu'elles sont définies dans la législation européenne pertinente :

Type de violation	Exemplification
Blanchiment de capitaux	Toute conversion ou transfert de biens, réalisés dans la certitude que ces biens sont issus d'une activité criminelle ou de la participation à une telle activité, dans le but d'occulter ou de dissimuler l'origine illicite de ces biens ou d'aider toute personne impliquée dans une telle activité à se soustraire aux conséquences juridiques de ses actes.
Détournement de fonds publics	Toute utilisation ou présentation de fausses déclarations ou de faux documents dans le but de bénéficier des contributions ou des financements accordés ou versés par les institutions européennes. Toute omission d'informations pertinentes dans le but de bénéficier des contributions ou des financements accordés ou versés par les institutions européennes.
Corruption active	Promettre ou remettre de l'argent à des agents publics, des clients ou des partenaires commerciaux.

Type de violation	Exemplification
	Promettre ou offrir des cadeaux ou des récompenses à des agents publics, des clients ou des partenaires commerciaux dont la valeur totale ne peut être qualifiée de modeste.
Comportement visant à ne pas payer la taxe sur la valeur ajoutée	Toute émission de factures ou d'autres documents pour des transactions même partiellement inexistantes afin de ne pas payer la TVA.
Contrebande	Toute soustraction de marchandises au contrôle douanier. Toute déclaration de données fausses ou incorrectes afin de ne pas payer ou de payer moins de droits de douane.

iii. Tous les actes ou omissions concernant le marché intérieur, y compris les violations des règles de l'UE en matière de concurrence et d'aides d'État, ainsi que les violations du marché intérieur liées à des actes contraires aux normes en matières de fiscalité des entreprises ou à des mécanismes dont le but est d'obtenir un avantage fiscal qui va à l'encontre de l'objet ou de la finalité de la législation applicable en matière de fiscalité des entreprises.

La présente procédure permet aux lanceurs d'alerte de faire un signalement anonyme, à condition qu'il soit étayé et documenté de manière adéquate. En conséquence, les signalements affectés par la généralité, l'approximation ou qui résultent de simples plaintes ne seront pas traités.

La loi sur le *signalement des lanceurs d'alerte* exclut du champ d'application de la procédure :

a. toute contestation, revendication ou demande liée à un intérêt personnel du lanceur d'alerte ou de la personne qui fait un signalement aux autorités judiciaires ou comptables, qui se rapportent exclusivement à son travail individuel ou à ses relations d'emploi public, ou liées à son travail ou à ses relations d'emploi public avec des personnalités hiérarchiquement supérieures ;
b. toute violation de la sécurité nationale, ainsi que des marchés publics liés à la défense ou à la sécurité nationale, à moins que ces aspects ne soient couverts par le droit dérivé pertinent de l'Union européenne ;
c. les communications de nature commerciale.

2.2.2. Contenu du signalement

Le signalement doit être circonstancié et fondé sur des éléments précis et concordants. **Il est rappelé aux auteurs de signalement que les informations communiquées doivent rester factuelles et présenter un lien direct avec l'objet de l'alerte.** Ces dernières ne doivent pas relever du secret de la défense nationale, du secret médical, du secret des délibérations judiciaires, du secret de l'enquête ou de l'instruction judiciaire ou du secret professionnel de l'avocat.

Dans la mesure du possible, le lanceur d'alerte doit présenter :

- une description claire et complète des faits qui font l'objet du signalement ;
- une indication des circonstances temporelles et géographiques dans lesquelles le fait faisant l'objet du signalement s'est produit ;
- les éléments permettant d'identifier la (les) personne(s) signalée(s) (par exemple, le titre, le lieu de travail où l'activité est exercée) ;
- tout document à l'appui de son signalement ;
- toute autre information utile pour vérifier l'existence des faits signalés.

Les motifs qui ont motivé le lanceur d'alerte à procéder au signalement ou à la divulgation publique ne sont pas pertinents pour le traitement du signalement et la protection contre les représailles.

2.3. **Canaux de signalement**

2.3.1. Canaux de signalement internes

Les signalements peuvent être effectués sous forme écrite ou orale par le biais des canaux énumérés ci-après :

- une plateforme informatique dédiée, accessible à partir du site web www.sofidel.com qui prévoit :
    - la possibilité de faire un signalement écrit en remplissant les formulaires prévus à cet effet ;
    - la possibilité de faire un signalement oral par le biais d'un système de messagerie vocale ;
- la demande, via la plateforme informatique dédiée, de la part du lanceur d'alerte d'une réunion avec le responsable du signalement, à laquelle peuvent également assister, à la demande du lanceur, d'éventuels facilitateurs, à fixer dans un délai de dix jours ouvrables à compter de la date de réception de la demande, et qui doit se tenir :

- dans les locaux de l'entreprise, en garantissant la pleine confidentialité du lanceur d'alerte ;

- sous réserve du consentement du lanceur d'alerte, par le bais de la vidéoconférence en mesure de garantir la plus grande confidentialité de l'entretien et à laquelle seules les personnes autorisés à y participer peuvent prendre part.

Sous réserve de l'accord du lanceur d'alerte, le signalement présenté oralement au cours de la réunion est documenté par le responsable du signalement sous forme d'enregistrement sur un support adapté au stockage et à l'écoute, ou sous forme de procès-verbal, qui peut être vérifié, modifié et approuvé par le lanceur d'alerte au moyen de sa signature.

Si le signalement interne est soumis par un canal autre que ceux expressément mentionnés, le destinataire doit transmettre ledit signalement sans délai (et au plus tard dans les sept jours suivant sa réception) au responsable du signalement, en informant simultanément le lanceur d'alerte de la transmission. L'anonymat ne peut pas toujours être garanti dans ce cas.

2.3.2. Canaux de signalement externes

Sans préjudice de la préférence pour le canal de signalement interne, le lanceur d'alerte ne peut présenter de signalement externe que si l'une des conditions suivantes est remplie lors de la présentation du signalement externe :

a. le canal de signalement interne n'est pas prévu dans le contexte de travail du lanceur d'alerte, c'est-à-dire que ce canal, même s'il est obligatoire, n'est pas actif ou, même s'il est activé, n'est pas conforme à la loi sur le signalement de *violation du droit de l'Union Européenne* ;

b. le lanceur d'alerte a déjà fait un signalement interne qui n'a pas été pris en compte ;

c. le lanceur d'alerte a des raisons fondées de croire que, s'il adresse un signalement interne, celui-ci ne sera pas suivi de manière efficace ou qu'il risque de faire l'objet de représailles ;

d. le lanceur d'alerte a des motifs raisonnables de croire que la violation peut constituer un danger imminent ou évident pour l'intérêt public.

Le signalement externe peut être adressé :

-à l'une des autorités listées en annexe du décret n° 2022-1284, choisie en fonction du domaine concerné par l'alerte ;

-au Défenseur des droits, soit directement habilité à recevoir un signalement, soit comme support à l'identification de l'autorité la mieux placée pour recevoir le signalement, compte tenu de son objet, lequel est joignable :

- par courrier gratuit, sans affranchissement, à l'adresse : Défenseur des droits – Libre réponse 71120 – 75342 Paris CEDEX 07 ;

- en renseignant le formulaire en ligne, sur : defenseurdesdroits.fr / « Saisir le Défenseur des droits » ;
- par téléphone, au 09 69 39 00 00, du lundi au vendredi de 8h30 à 19h30.

-à l'autorité judiciaire ;

-à une institution, un organe, ou un organisme de l'Union européenne, si le signalement porte sur une violation relevant du champ d'application de la directive 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019.

2.3.3. Divulgation publique

Sans préjudice de la préférence pour le canal de signalement interne et de la possibilité d'utiliser, en présence des conditions précitées, les canaux de signalement externes, le lanceur d'alerte peut effectuer une divulgation publique, en bénéficiant de la protection prévue par la loi sur la violation du droit de l'Union Européenne, uniquement si, au moment de la présentation de ladite divulgation :

- le lanceur d'alerte a déjà effectué un signalement interne et externe ou a adressé directement un signalement externe, si les conditions nécessaires étaient remplies, sans avoir de réponse dans le délai prévu par le décret relatif aux signalement des violations du droit de *l'Union Européenne* sur les mesures envisagées ou adoptées pour donner suite aux signalements ;

- dans le cas où le lanceur d'alerte estime qu'il peut y avoir un danger grave et imminent (par exemple en cas de situation d'urgence ou de risque de dommages irréversibles), pour les signalements portant sur des informations obtenues dans le cadre professionnel ;

- lorsque le lanceur d'alerte estime qu'il existe un risque de représailles en cas de signalement à l'autorité extérieure, ou que cette même autorité ne traite pas efficacement le signalement dans le cas en question, en raison du risque de destruction ou de dissimulation de preuves, ou parce que l'autorité est peut-être de connivence avec l'auteur de la violation voire impliquée dans cette infraction.

2.4. Gestion du signalement

Le rôle de gestionnaire du signalement reçu par le biais du canal de signalement interne spécifiquement mis en place par Sofidel France est confié au Country Human Resources Manager, qui traite les signalements internes reçus de manière confidentielle, en protégeant le lanceur d'alerte et ses collaborateurs, ainsi que l'honneur et l'identité du lanceur d'alerte.

Si le signalement se réfère au Gestionnaire du signalement, le lanceur d'alerte peut le transmettre à la Commission Whistleblowing spécifiquement établie au sein de SOFIDEL S.p.A. et composée du directeur des ressources humaines, du directeur de la gestion des risques et de la conformité et du directeur de l'audit interne, afin d'évaluer de manière appropriée les mesures à prendre.

Le processus de gestion des signalements se divise en cinq phases détaillées ci-dessous, chacune d'entre elles devant faire l'objet d'une documentation adéquate :

a. évaluation préliminaire ;

b. enquête préliminaire ;

c. décision ;

d. conservation de la documentation

e. *reporting* et suivi des mesures de correction.

Le lanceur d'alerte a la possibilité, de vérifier à tout moment l'état d'avancement de son signalement, ainsi que l'issue de la procédure (y compris l'archivage) en accédant à la plateforme.

a) Évaluation préliminaire

Le gestionnaire préposé traite les signalements de manière confidentielle, en adoptant des procédures appropriées afin de protéger le lanceur d'alerte, son identité et son honneur, ainsi que ceux de toute autre personne impliquée.

Ce même gestionnaire fait une évaluation préliminaire du signalement, en veillant à ce qu'il soit traitée de manière appropriée, et en particulier :

- dans un délai de sept jours à compter de la date de réception du signalement, il délivre au lanceur d'alerte, par le biais de la plateforme informatique dédiée, l'accusé de réception de ce signalement ;

- Vérifie que le signalement est suffisamment détaillé pour pouvoir être évalué, en restant en contact avec le lanceur d'alerte au cas où des compléments seraient nécessaires, et en déterminant également si ce même signalement relève du champ d'application de la législation sur les signalement de *violations du droit de l'Union européenne* ;

- classe le signalement en notifiant le lanceur d'alerte et en formalisant par écrit les raisons de la décision du classement :

    1. qui ne relèvent pas du champ d'application de la présente procédure, en les transmettant, si nécessaire, à d'autres départements/fonctions d'entreprise de compétence (par exemple, dans le cas de plaintes) ;

    2. si, dans un délai de 30 jours ouvrables à compter de la demande, le lanceur ne présente pas les informations supplémentaires demandées ou les fournit de manière non exhaustive et/ou, insuffisante pour permettre une évaluation complète du signalement

    3. si elles sont manifestement infondées ou de mauvaise foi, ou dont le contenu est si général qu'il rend impossible un suivi diligent du signalement.

- Si le signalement est suffisamment détaillé, il passe à l'étape b).

b) Enquête préliminaire

Si, à l'issue de l'évaluation préliminaire, le gestionnaire des signalements estime que le signalement est bien fondé en ce sens qu'il est suffisamment étayé et accompagné de preuves, il/elle

- classe le signalement ;
- mène des activités de vérification spécifiques (par exemple, l'analyse de documents, les entretiens et enquêtes internes) en collaborant, le cas échéant, avec les fonctions de l'entreprise compétentes eu égard à l'objet du signalement et des organismes de contrôle ou des consultants/professionnels externes pour les enquêtes spécifiques et spécialisés. Si des consultants ou des professionnels externes sont engagés, il est nécessaire d'inclure dans le contrat d'assistance conclu avec eux une clause de sauvegarde de la confidentialité des informations partagées, indiquant précisément les types d'informations et/ou de documents qui doivent rester secrets (NDA) ;
- examine les circonstances en analysant les documents et les données disponibles et, s'il le juge nécessaire, interroge le lanceur d'alerte et d'autres personnes susceptibles de rapporter les faits qui font l'objet du signalement. Ces activités doivent être documentées par l'enregistrement de la réunion ou par la rédaction d'un procès-verbal de la réunion, qui doit être signé par le lanceur d'alerte ou d'autres personnes impliquées pour approbation ;
- suspend l'enquête préliminaire s'il estime, au terme des investigations approfondies menées, y compris avec la possible participation d'autres structures de l'entreprise ou de consultants/professionnels externes, que le signalement n'est pas fondé, en prenant soin de formaliser les raisons à l'appui d'une telle décision ;
- fournit un retour d'information diligent au lanceur d'alerte, si ce dernier demande à être tenu au courant de l'évolution de l'affaire.

Au cours de la phase d'enquête préliminaire, le gestionnaire des signalements garantit :

- l'impartialité, l'équité et l'exactitude de l'analyse et de l'évaluation du signalement interne ;
- la confidentialité des informations collectées et la confidentialité de l'identité du lanceur d'alerte, le cas échéant ;
- la non-utilisation des signalements internes au-delà de ce qui est nécessaire pour en assurer un suivi adéquat.

Le responsable des signalements ne peut partager avec les fonctions, les organismes de contrôle et les professionnels concernés que les informations strictement nécessaires à l'exercice de ses activités, et ne peut divulguer l'identité du lanceur d'alerte, si elle est connue, qu'avec le consentement explicite de ce dernier. Sans ledit consentement, le gestionnaire des signalements ne peut partager aucune information, aucun fait ou aucune preuve susceptible de permettre l'identification du lanceur d'alerte.

Dans les trois mois à partir de la date de l'accusé de réception ou, à défaut, dans un délai de trois mois à compter de l'expiration du délai de sept jours à compter de la soumission du signalement, le gestionnaire des signalements fournit un retour d'information au lanceur d'alerte, par l'intermédiaire de la plateforme informatique prévue à cet effet, sur les suites déjà données ou à donner à son signalement. Le retour d'informations peut être définitif si l'enquête a été menée à bien, ou de nature provisoire sur son état d'avancement si l'enquête est toujours en cours. Dans ce dernier cas, le responsable des signalements communiquera par la suite le résultat final de l'enquête préliminaire.

c) Décision

À l'issue de la phase d'enquête préliminaire, le gestionnaire des signalements peut prendre les décisions suivantes :

- classement sans remarques :
- recommandation de mesures de correction (par exemple, sessions de formation, initiative de communication, changements organisationnels, mises à jour des procédures, audits), en coordination avec toute autre fonction compétente ;
- évaluation de toute mesure disciplinaire, conformément à la législation en vigueur, aux conventions collectives nationales de travail et aux règles internes, en impliquant les fonctions compétentes ;
- une information en temps utile au Représentant légal et, pour les signalements en matière de corruption, au Focal Point de Sofidel France (c'est-à-dire le Manager en charge de la gestion du système anti-corruption), ainsi qu'aux fonctions/entités compétentes, compte tenu de l'objet du signalement, dans la mesure où l'affaire en question l'exige pour évaluer correctement toute mesure à prendre dans le cadre de ses compétences.

Une fois la décision formalisée, le gestionnaire des signalements consolide un rapport d'enquête dans lequel il illustre :

- le contenu du rapport et, le cas échéant, de toute documentation à l'appui ;
- l'activité d'enquête préliminaire menée, en présentant une reconstitution chronologique exhaustive de celle-ci ;
- les constatations et les preuves collectées à l'appui ou non du signalement, en illustrant clairement les informations nécessaires à l'évaluation de l'affaire ;
- les conclusions, indiquant si le comportement signalé constitue une violation, qu'elle soit prouvée ou non (ou si les preuves collectées étaient insuffisantes) et, si le fait a été établi, en proposant les mesures à prendre.

d) Conservation de la documentation

Sauf disposition légale ou réglementaire contraire :

- Les données relatives à une alerte peuvent être conservées en base active jusqu'à la prise de la décision définitive sur les suites à réserver à celle-ci. Cette décision interviendra dans un délai raisonnable à compter de la réception du signalement.
- Après la prise de la décision définitive sur les suites à réserver à l'alerte, les données pourront être conservées sous forme d'archives intermédiaires, le temps strictement proportionné à leur traitement et à la protection de leurs auteurs, des personnes qu'ils visent et des tiers qu'ils mentionnent, en tenant compte des délais d'éventuelles enquêtes complémentaires. Elles pourront également être conservées pour une durée plus longue sous forme d'archives intermédiaires si Sofidel en a l'obligation légale (par exemple, pour répondre à des obligations comptables, sociales ou fiscales), ou à des fins probatoires dans l'optique d'un contrôle ou d'un contentieux éventuel, ou encore à des fins de réalisation des audits de qualité des processus de traitement des signalements.
- Lorsqu'une procédure disciplinaire ou contentieuse est engagée à l'encontre d'une personne mise en cause ou de l'auteur d'une alerte abusive, les données relatives à l'alerte peuvent être conservées par l'organisation chargée de la gestion des alertes jusqu'au terme de la procédure ou de la prescription des recours à l'encontre de la décision intervenue.

e) Reporting et suivi des mesures d'action.

Le gestionnaire du signalement formalise par écrit, dans le rapport final approprié, les évaluations et les décisions prises, les informations fournies lorsque l'affaire l'exige spécifiquement et les recommandations et propositions (le cas échéant) pour l'application de mesures disciplinaires, en procédant également à leur classement sur la plateforme, afin d'assurer la traçabilité, la confidentialité, la préservation et la récupération des données tout au long de la procédure.

Il incombe aux responsables des fonctions/processus concernés par le signalement de mettre en œuvre les recommandations reçues par le gestionnaire du rapport et les mesures de correction identifiées, même avec les soutiens professionnels externes, si disponibles.

Le responsable des signalements surveille la mise en œuvre des recommandations et des mesures de correction, en présentant des mises à jour périodiques au représentant légal et, pour les signalements en matière de corruption, au Focal point de Sofidel France, ainsi qu'aux fonctions/entités compétentes lorsque le cas l'exige.

2.5. Protection des personnes physiques impliquées dans le processus de signalement

2.5.1. Protection du lanceur d'alerte et des collaborateurs assimilés

Le système de protection des lanceurs d'alerte s'applique également aux différentes personnes qui pourraient subir des représailles, même indirectes, en raison de leur rôle dans le processus d'alerte,

de divulgation publique ou de plainte, ainsi que de la relation particulière qu'elles entretiennent avec le lanceur d'alerte. et notamment :

- aux facilitateurs ;
- aux personnes liées au lanceur d'alerte qui risquent de faire l'objet de mesures de rétorsion dans le cadre de leurs activités professionnelles ;
- aux personnes morales (ex : syndicat) en lien avec le lanceur d'alerte et qui, par ricochet, peuvent être victimes de représailles en raison du signalement.

Le système de protection du lanceur d'alerte (et des personnes traitées comme telles) comprend par ailleurs les protections suivantes :

i. Protection de la confidentialité et des données personnelles

Dans le respect des principes fondamentaux sur la protection des données personnelles, tels que les principes de limitation des finalités et de minimisation des données, les signalements ne peuvent être utilisés au-delà de ce qui est nécessaire pour leur donner une suite adéquate.

Le personnel de Sofidel France qui reçoit un signalement et/ou qui est impliqué de quelque manière, dans la gestion du signalement, est tenu de garantir la plus stricte confidentialité sur l'identité des personnes (lanceurs d'alertes ou personnes assimilées, et personnes concernées), sur toute information permettant de déduire directement ou indirectement cette identité, et sur les faits signalés, sauf dans les cas où :

- le lanceur d'alerte consent à la divulgation de ces informations à des personnes autres que les personnes compétentes ;
- dans le cadre des procédures de signalement internes et externes, la divulgation de l'identité du lanceur d'alerte est indispensable, notamment aux fins de sa défense, lorsqu'il a donné son consentement exprès à la divulgation de son identité et a notifié par écrit les raisons de la divulgation de son identité.
- dans le cadre de la procédure disciplinaire engagée à l'encontre de la personne signalée, si l'identité du lanceur d'alerte est indispensable à sa défense, sous réserve du consentement exprès du lanceur d'alerte à la divulgation de son identité et de la communication préalable par écrit des raisons motivant la divulgation de son identité.

La violation de l'obligation de confidentialité est source de responsabilité disciplinaire, sans préjudice de toute autre responsabilité (notamment pénale) prévue par la loi. Les données personnelles qui ne sont manifestement pas utiles au traitement d'un signalement spécifique ne sont pas collectées ou, si elles le sont accidentellement, leur suppression est immédiate.

Le modèle de réception et de traitement des signalements doit faire l'objet d'une analyse d'impact sur la protection des données (DPIA, *Data Protection Impact Assessment*, ex art. 35 RGPD) afin

d'identifier et d'adopter les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque CID (confidentialité, intégrité et disponibilité).

ii. Protection contre toute mesure de représailles, même si elle n'est que tentée ou menacée par l'entreprise, en raison du signalement, de la divulgation publique ou de la plainte.

Le statut de lanceur d'alerte confère une protection contre les mesures de représailles, notamment disciplinaires, qui prendraient notamment l'une des formes suivantes : suspension, mise à pied, licenciement, rétrogradation ou refus de promotion, transfert de fonctions, changement de lieu de travail, réduction de salaire, mesures disciplinaires, discriminations, etc.

Pour que le lanceur d'alerte bénéficie de cette protection, il doit y avoir un lien étroit entre le signalement, la divulgation publique, la plainte et le comportement, l'acte ou l'omission défavorable qui cause, a causé ou peut causer, directement ou indirectement, un préjudice injustifié.

Le lanceur d'alerte peut communiquer à l'autorité judiciaire les représailles qu'il estime avoir subies, pour des mesures relevant de sa compétence. L'autorité judiciaire adopte également les mesures, même provisoires, nécessaires pour assurer la protection de la situation juridique subjective mise en place (par exemple, réparation des dommages, réintégration sur le lieu de travail, injonction de cesser les représailles et la déclaration de nullité des actes entrepris en tant que représailles).

Aucune protection n'est garantie s'il est établi, même par un jugement de première instance, que le lanceur d'alerte est pénalement responsable des délits de diffamation ou de calomnie, ou en tout cas des mêmes délits commis lors d'une plainte auprès de l'autorité judiciaire ou comptables, ou qu'il est civilement responsable en cas de faute intentionnelle ou de négligence grave. Dans ce cas, une sanction disciplinaire est prononcée à l'encontre du lanceur d'alerte ou de la personne qui a porté plainte.

Dans le cadre de procédure judiciaire ou administrative, ou dans tous les cas de litiges extrajudiciaires concernant la détermination des comportements, actes ou omissions interdits envers le lanceur d'alerte (ou des personnes assimilées à ce rôle) ; les mêmes actes sont présumés avoir été accomplis en raison du Rapport, de la Divulgation publique ou de la plainte auprès des autorités judiciaires ou comptables. Il incombe à la personne qui a accompli ces actes de prouver qu'ils sont motivés par des raisons étrangères.

iii. Limitations de la responsabilité civile et pénale

Le lanceur d'alerte bénéficie, sous certaines conditions, d'une limitation de sa responsabilité civile. Cela signifie que si la personne mise en cause par son alerte subit des préjudices en conséquence de son signalement, le lanceur d'alerte ne peut être condamné à réparer ces préjudices. Néanmoins, pour bénéficier de cette exonération, le lanceur d'alerte doit avoir respecté les conditions suivantes :

- Son alerte doit avoir été réalisée dans le respect des règles posées par les textes ;
- Le lanceur d'alerte doit avoir des motifs raisonnables de croire que le signalement ou la divulgation de l'intégralité des informations était nécessaire à la sauvegarde des intérêts en cause.

La responsabilité pénale du lanceur d'alerte ne peut être engagée si, par son alerte ou pour pouvoir lancer celle-ci :

- Le lanceur d'alerte a porté atteinte à un secret protégé par la loi (ex. : secret professionnel, secret des correspondances), étant précisé que l'irresponsabilité pénale ne joue pas pour les secrets protégés exclus du régime de l'alerte (ex. 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 lanceur d'alerte a soustrait, détourné ou recelé des documents ou tout autre support contenant des informations auxquels il a eu accès de manière licite.

Pour être pénalement protégé, le lanceur d'alerte doit avoir respecté deux conditions, à savoir :

- Son alerte doit avoir été réalisée dans le respect des règles posées par les textes ;
- La divulgation des informations doit être nécessaire et proportionnée à la sauvegarde des intérêts en cause.

En tout état de cause, la responsabilité pénale et toute autre responsabilité, y compris la responsabilité civile, n'est pas exclue en cas de comportement, d'acte ou d'omission sans rapport avec le signalement ou qui n'est pas strictement nécessaire pour divulguer la violation.

2.5.2. Mesures de protection à l'égard de la personne concernée et des autres personnes impliquées dans le signalement

La protection de l'intégrité et de la confidentialité s'étend également aux personnes concernées par le signalement, ainsi qu'à toute tierce partie mentionnée dans ce dernier.

Si, à la suite des retours d'informations concrets concernant le signalement, le responsable compétent poursuit l'activité d'enquête, la personne concernée peut être contactée et se verra offrir la possibilité de fournir toute clarification nécessaire.

La personne concernée n'a pas le droit d'obtenir des informations sur l'origine du signalement, ni de recevoir des informations sur les données personnelles de la personne concernée.

La protection de la personne concernée s'applique sans préjudice des dispositions de la loi imposant l'obligation de communiquer le nom de la personne concernée comme étant soupçonnée d'être responsable de la violation (par exemple, les demandes de l'autorité judiciaire).

Le comportement de tout lanceur d'alerte qui est l'auteur de signalements non fondés avec une faute intentionnelle ou une négligence grave est également sanctionné.

Tout abus de cette procédure, y compris les signalements internes manifestement opportunistes et/ou rédigés dans le seul but de nuire à la personne concernée ou à d'autres personnes impliquées dans le

signalement, est une source de responsabilité face aux instances disciplinaires et autres instances compétentes.

2.6. Mise en œuvre effective de la procédure

Le représentant légal de Sofidel France supervise la mise en œuvre effective de cette procédure, tout en assurant :

- l'activation du canal d'alerte interne, en pourvoyant les ressources nécessaires à l'adoption et à la maintenance de la plateforme informatique dédiée ;

- la mise en place d'activités de formation spécifiques appropriées pour les membres du Gestionnaire des signalement ainsi que pour les lanceurs d'alerte potentiels ayant une relation de travail avec Sofidel France.

2.7. Diffusion de la procédure et rapport sur le fonctionnement des canaux internes

Afin d'encourager l'utilisation du système d'alerte interne et de favoriser la diffusion d'une culture de la légalité, la procédure est publiée dans son intégralité sur le site internet prévu à cet effet où sont publiées les procédures de la société.

Le gestionnaire des signalements rend compte chaque semestre du bon fonctionnement des canaux internes de dénonciation, en indiquant dans un rapport les informations globales sur les résultats de l'activité menée directement et sur les suites données aux signalements reçus. Ce reporting est établi dans le respect des règles relatives à la protection des données à caractère personnel. Le responsable des signalements envoie le rapport susmentionné au représentant légal.

En outre, un flux d'informations, automatisé si nécessaire, vers la Commission Whistleblowing de la société mère, contenant des informations agrégées sur les résultats des activités menées est envisagé, comme outil indispensable pour toute activité de contrôle et de vérification.

3. Listes des modules

Aucun module n'est joint

4. Classement

DOCUMENT	RESPONSABLE	FORMAT	PÉRIODE DE CLASSEMENT
Rapport final et tous les documents relatifs au signalement	Gestionnaire des signalements	Électronique	Voir le point « d » du paragraphe 2.4

5. Définitions

- **Contexte professionnel :** le travail ou les activités professionnelles, passées ou présents, exercés dans le cadre des relations de travail, par lesquels, indépendamment de la nature de ces activités, une personne obtient des informations sur des violations et dans le cadre desquels elle peut risquer de subir des représailles en cas de divulgation publique ou de signalement aux autorités judiciaires ou comptables ;

- **Divulgation publique** : communication dans le domaine public d'informations sur des violations par le biais de la presse ou des médias électroniques ou encore par des moyens de diffusion susceptibles d'atteindre un grand nombre de personnes ;

- **Facilitateur** : une personne physique qui aide un lanceur d'alerte au cours du processus de signalement, qui opère dans le même contexte professionnel et dont l'aide doit rester confidentielle ;

- **Gestionnaire des signalements** : une personne physique ou un bureau qui reçoit les rapports, les examine et prend toutes les initiatives jugées nécessaires en vérifier le bien-fondé ;

- **Informations sur les violations** : informations, y compris des soupçons fondés, concernant les violations commises ou qui, sur la base d'éléments concrets, pourraient être commises dans l'organisation avec laquelle le lanceur d'alerte ou l'auteur de la plainte auprès des autorités judiciaires ou comptables a un lien juridique, ainsi que les éléments concernant les comportements visant à dissimuler ces violations ;

- **Retour d'information** : communication au lancer d'alerte d'informations concernant la suite données ou envisagée à son signalement ;

- **Représailles** : tout acte ou omission ou comportement, y compris sous forme de tentative ou de menace, commis à la suite du signalement, de la plainte auprès de l'autorité judiciaire ou comptable ou d'une divulgation publique et qui cause ou peut causer, un préjudice injustifié, directement ou indirectement, à l'auteur de la plainte ;

- **Lanceur d'alerte** : la personne physique, auteur du signalement, soit par des voies de signalement internes, soit par des voies de signalement externes, ou la divulgation publique d'informations sur des violations acquises dans le cadre de son activité professionnelle ;

- **Personne concernée :** la personne physique ou morale mentionnée dans le signalement interne ou externe ou dans la divulgation publique en tant que personne à laquelle la violation est attribuée ou en tant que personne impliquée d'une manière ou d'une autre dans la violation signalée ou divulguée publiquement ;

- **Signalement ou signaler :** la communication orale ou écrite d'informations sur les violations ;

- **Signalement anonyme** : Signalement sans les éléments permettant d'identifier le lanceur d'alerte ;

- **Signalement interne** : la communication, écrite ou orale, d'informations sur des violations, soumises par le biais du canal de signalement interne ;

- **Signalement externe** : la communication, orale ou écrite, d'informations sur des violations, par le biais du canal de signalement externe mis en place par l'autorité nationale compétente ;

- **Suivi** : toute mesure pris par le gestionnaire du canal de signalement pour évaluer l'exactitude des allégations signalées, le résultat de l'enquête et les éventuelles mesures prises ;

- **Tiers :** collaborateurs, les professions libérales, consultants, fournisseurs, clients et plus généralement toute personne qui a nouée une relation d'intérêt avec Soffass, qu'elle soit rémunérée ou non ;

- **Violations** : comportement, actes ou omissions qui va à l'encontre de l'intérêt public ou à l'intégrité de l'administration publique ou de l'entité privée.