
PROCEDURE DISPOSITIF D'ALERTE INTERNES

REFERENCE

Type de PROCEDURE
document :

Centre : TOUS

Client : TOUS

Référence : SMC-PR-03-Procédure
Dispositif d'Alertes Internes

Version : 3.1

Niveau de
classification C2-Interne

Destinataires Tous les acteurs du groupe TESSI

Copies Clients sur demande.

ETAT DES VERSIONS SUCCESSIVES

N°	DATE	Observations	Rédigé par	Vérifié par	Approuvé par
1.0	25/08/2017	Création	S. METRAL-CHARVET	A. GERELLI	C. MUTEL F. DUFFAUD
2.0	14/05/2019	Mise à jour charte graphique et ajout applicabilité à l'international	S. METRAL-CHARVET	A. GERELLI	C. MUTEL F. DUFFAUD
2.1	04/09/2019	Correction	S. METRAL-CHARVET	A. GERELLI	C. MUTEL F. DUFFAUD
3.0	30/08/2021	Evolution de dispositif d'alerte interne	A. TALBI	P. PEILLON	O. JOLLAND
4.0	10/10/2022	Intégration spécificités loi WASERMAN	A. TALBI	P. PEILLON	O. JOLLAND

Procédure Dispositif d'Alertes Internes

Sommaire

1. Description de la procédure	4
1.2 OBJET	4
1.3 DOMAINE D'APPLICATION	4
2. CONFIDENTIALITÉ ET SÉCURITÉ DE TRAITEMENT – DONNÉES COLLECTÉES	6
3. LES DIFFERENTS TYPES DE REFERENTS POUR LES ALERTES	6
4. LOGIGRAMME DU TRAITEMENT D'UNE ALERTE	8
5. TRAITEMENT DE L'ALERTE	9
5.1 EMETTRE L'ALERTE	9
ACCUSE DE RECEPTION ET ANALYSE DE L'ALERTE	10
MENER DES VERIFICATIONS APPROFONDIES	10
DECIDER ET TRAITER L'ALERTE	10
6. DURÉE DE CONSERVATION DES DONNÉES	11
7. DESTINATAIRES DES DONNEES ET SOUS-TRAITANTS	12
8. INFORMATION DES PERSONNES	12
9. DROIT DES PERSONNES CONCERNEES	12
10. MESURES DE SECURITE	13

1. DESCRIPTION DE LA PROCEDURE

1.2 OBJET

L'objet de cette procédure est de décrire l'organisation, les moyens et les modalités de traitements des soumissions des alertes internes pour répondre aux exigences de la loi SAPIN II, la loi relative devoir de vigilance et le Code d'éthique du Groupe Tessi.

1.3 DOMAINE D'APPLICATION

Conformément aux dispositions réglementaires françaises auxquelles le Groupe doit se conformer y compris dans ses filiales internationales et conformément au code éthique du Groupe Tessi, le dispositif d'alerte interne décrit dans la présente procédure permet de demander conseil en matière d'éthique et de signaler des délits, ou des comportements contraires au code dans les domaines suivants :

- Financier, comptable et bancaire,
- Lutte contre la corruption,
- Lutte contre les pratiques anticoncurrentielles,
- Lutte contre les discriminations et le harcèlement au travail,
- Santé, hygiène et sécurité au travail,
- Protection de l'environnement.

1.3.1 EN APPLICATION DE LA LOI SAPIN II

Le dispositif d'alerte interne mis en place par le Groupe vise à permettre aux employés de signaler des conduites ou des situations contraires au Code Ethique du Groupe, susceptibles de caractériser des faits de corruption ou de trafic d'influence.

Il permet également aux membres du personnel et aux collaborateurs extérieurs et occasionnels de signaler :

- Un crime ou un 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 graves pour l'intérêt général, dont l'émetteur de l'alerte a eu personnellement connaissance.

La base légale du traitement d'Alerte Interne est l'obligation légale.

La liste des personnes susceptibles d'être qualifiées de lanceurs d'alerte a été fixée par l'article 8-I de la loi Sapin 2, modifié par l'article 3 de la loi du 21 mars 2022. Il s'agit :

- Des salariés, anciens salariés et candidats à un emploi ;

- Des actionnaires, associés et titulaires de droits de vote au sein de l'assemblée générale de l'entreprise ;
- Des membres de l'organe d'administration, de direction ou de surveillance ;
- Des collaborateurs extérieurs et occasionnels ;
- Des co-contractants de l'entreprise, de leurs sous-traitants ou, s'il s'agit de personnes morales, des membres de l'organe d'administration, de direction ou de surveillance, ainsi que des salariés de ces co-contractants et de ces sous-traitants.

Le cercle des personnes pouvant procéder à des signalements est donc très large, et ce d'autant plus que l'auteur du signalement peut être une personne nommément désignée ou anonyme.

1.3.2 EN APPLICATION DE LA LOI RELATIVE AU DEVOIR DE VIGILANCE

Le dispositif d'alerte interne du Groupe vise à 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 du Groupe et de celles des filiales qu'elle contrôle directement ou indirectement, ainsi que des activités des sous-traitants ou fournisseurs avec lesquels est entretenue une relation commerciale établie, lorsque ces activités sont rattachées à cette relation.

La base légale du traitement d'Alerte Interne est l'obligation légale.

1.3.3 EN CAS DE FRAUDE

Le dispositif d'alerte interne permettant le recueil de tout signalement de type fraude ou suspicion de fraude, quel que soit l'auteur de l'alerte ou son lien avec le Groupe.

« On qualifie de fraude, toute action destinée à tromper ou tout acte réalisé en utilisant des moyens déloyaux, en vue d'obtenir un avantage matériel ou moral indu ou réalisé avec l'intention d'échapper à l'application de la loi, des procédures, des politiques et des bonnes pratiques formalisées du Groupe.

La falsification, la malversation, l'abus, le détournement, l'escroquerie, le trucage, la tromperie, la dissimulation sont des exemples de fraude ».

A titre d'exemple, les risques de Fraude ont ainsi été classifiés en plusieurs grands domaines :

- Fraudes bancaires ;
- Fraudes commerciales ;
- Fraude sur les moyens de paiement
- Fraudes sur les salaires / primes ;
- Fraudes téléphoniques ;
- Vol de données personnelles.

La base légale de ce traitement est de l'intérêt légitime de Tessi.

2.CONFIDENTIALITÉ ET SÉCURITÉ DE TRAITEMENT – DONNÉES COLLECTÉES

Conformément à la réglementation en matière de protection du lanceur d'alerte, le traitement d'une alerte garantit la plus stricte confidentialité de l'émetteur, des personnes visées, de tout tiers qui est mentionné, et des informations recueillies. Toutes les personnes intervenant dans le traitement des alertes sont astreintes à une obligation de confidentialité renforcée.

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

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

Les informations recueillies ne peuvent être communiquées à des tiers que si cette communication est nécessaire pour traiter le signalement et dans le respect de la confidentialité des informations recueillies.

Les accès au traitement des données collectées au moyen du dispositif d'alerte s'effectuent par des mots de passe individuels qui sont régulièrement modifiés. Ces accès sont enregistrés et leur régularité est contrôlée.

Seules les données suivantes peuvent être traitées dans le cadre du dispositif :

- Identité, fonctions et coordonnées de l'émetteur 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 ;
- Eléments recueillis dans le cadre de la vérification des faits signalés,
- Compte-rendu des opérations de vérification,
- Suites données à l'alerte ;

Des alertes anonymes seront également traitées dans le cadre de cette procédure, selon les obligations réglementaires locales propres à chaque pays et dans la mesure où la gravité des faits mentionnés est établie et les éléments factuels sont suffisamment détaillés pour en permettre le traitement ;

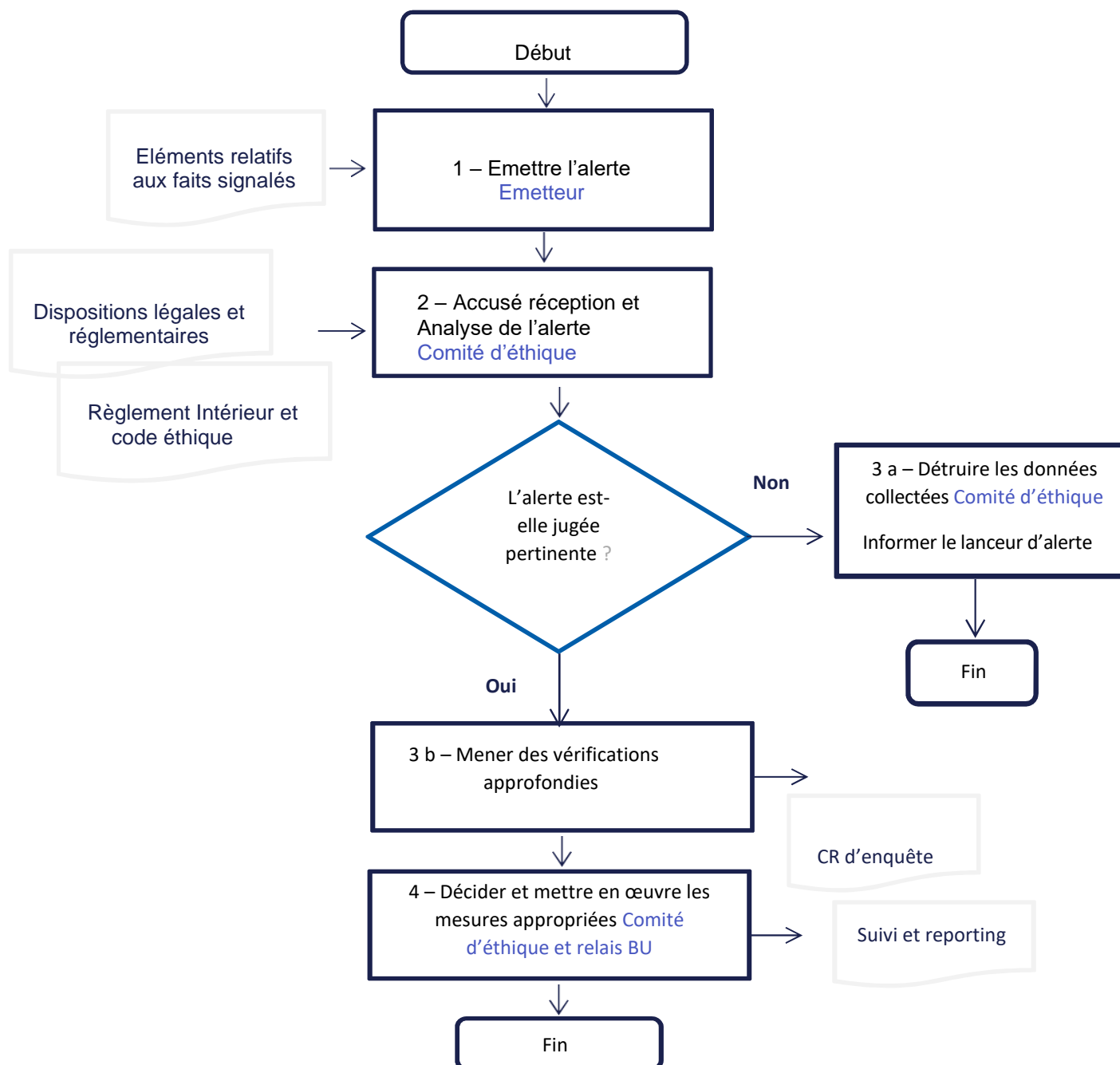
3.LES DIFFERENTS TYPES DE REFERENTS POUR LES ALERTES

- **Le Référent principal** : est un membre du comité d'éthique, il reçoit et analyse les alertes lui ayant été signalées par tout moyen, et notamment via la plateforme, courrier, email, téléphone ou en personne. Il peut se faire assister de délégués. Il dispose de tous les droits et peut voir et agir sur toutes les signalements peu importe la catégorie. Il peut accéder à l'administration de la plateforme, inviter des utilisateurs, les supprimer.

Le Comité Ethique est composé des membres suivants :

- Directeur Juridique Groupe,
 - Directeur Compliance Groupe
 - Compliance Officer Groupe
 - Directeur RH Groupe
 - Directeur de l'audit interne Groupe
 - Responsable RSE du Groupe
-
- **Le Référent spécifique** : Il est responsable mais dédié exclusivement à une ou plusieurs catégories d'alertes prédéfinies, par exemple le DRH est en charge des Alertes RH, il dispose de toutes les fonctionnalités pour traiter les alertes de cette catégorie spécifique et ne voit pas les signalements et l'activité des autres catégories.
 - **Le Référent occasionnel** : Il n'est rattaché à aucune catégorie d'alerte mais peut créer des cas internes depuis sa session. Il peut être invité sur un cas par les référents principaux et spécifiques. Exemple : Relais Compliance d'une filiale.
 - **Le Contributeur occasionnel** : Il est une personne invitée par un référent sur un signalement pour ponctuellement traiter ou aider au traitement. Il accède à l'intégralité du signalement mais il n'a accès qu'à ce signalement et ne voit rien d'autre, il dispose de droits restreints, par exemple : ne peut pas inviter d'autres.

4. LOGIGRAMME DU TRAITEMENT D'UNE ALERTE



5. TRAITEMENT DE L'ALERTE

5.1 EMETTRE L'ALERTE

Tous les collaborateurs internes (salariés à temps plein, partiel, temporaire, apprentis et stagiaires) et collaborateurs externes ou occasionnels (y compris les sous-traitants ou fournisseurs ou partenaires commerciaux des filiales du Groupe) peuvent signaler une alerte sur la plateforme <https://tessi.signalement.net>

Les alertes saisies via la plateforme sont réceptionnées par les référents identifiés sur la plateforme de signalement.

La plateforme dite « signalement.net », disponible à l'adresse : <https://tessi.signalement.net> est un dispositif d'alertes professionnelles en ligne qui permet aux filiales du Groupe Tessi, d'une part, de se mettre en conformité avec ses différentes obligations légales et réglementaires et, d'autre part, de disposer d'un outil efficient de gestion de tout type de signalement interne.

L'utilisation de la plateforme est facultative, Tessi ne prendra aucune mesure à l'encontre de ceux qui utiliseraient un autre canal de signalement. En effet, la plateforme « signalement.net » n'a pas pour objet de se substituer aux voies habituelles de communication interne (téléphone, messagerie, visioconférence ou en présentiel) qui se font au travers de la structure hiérarchique (auprès du supérieur hiérarchique direct ou indirect), de la direction des Ressources Humaines, ou encore auprès d'un représentant du personnel. Elle a donc un caractère subsidiaire.

Par ailleurs, le lanceur d'alerte peut également choisir de procéder directement à un signalement externe, par exemple en saisissant une autorité judiciaire, le défenseur des droits ou une autorité administrative.

Le décret du 3 octobre 2022 de la loi Wasserman dresse la liste de ces « autorités compétences » en fonction du domaine de l'alerte. Par exemple, la CNIL est répertoriée pour les alertes relatives à la protection de la vie privée et des données personnelles, à la sécurité des réseaux et de systèmes d'information. La DGT est désignée pour les alertes relatives aux relations individuelles et collectives du travail, conditions de travail et la DGEFP pour les alertes relatives à l'emploi et la formation professionnelle.

Le signalement doit être fait de bonne foi, c'est-à-dire en ayant la croyance raisonnable et idéalement des preuves factuelles que les faits sont vrais au moment de leur signalement. L'utilisation abusive du dispositif est à proscrire.

L'auteur de l'alerte doit avoir eu connaissance des faits qu'il rapporte, directement ou indirectement.

Le signalement doit préciser en particulier :

- La date des faits
- L'identité des personnes impliquées lorsque ces éléments sont connus de l'auteur de l'alerte
- Les raisons de sa connaissance personnelle des faits, et si un tiers a été informé
- La description des faits avec des éléments venant les étayer
- L'identité et coordonnées de l'émetteur de l'alerte.

ACCUSE DE RECEPTION ET ANALYSE DE L'ALERTE

Par catégorie d'alerte, un référent principal a été désigné comme pilote de l'alerte.

Le pilote aura pour mission d'accuser réception des alertes, de proposer le plan d'action aux autres membres du comité d'éthique afin d'instruire le dossier de manière appropriée.

L'auteur de l'alerte recevra un accusé de réception de son signalement daté, en principe dans les 7 jours ouvrés suivant le signalement.

L'examen de la recevabilité de l'alerte s'effectue dans un délai raisonnable n'excédant pas en principe 60 jours ouvrés, après réception de l'alerte. L'auteur est tenu informé de sa recevabilité.

Cette étape permet d'éliminer rapidement les alertes hors champ d'application.

MENER DES VERIFICATIONS APPROFONDIES

Si le signalement est recevable, une enquête sera effectuée afin de déterminer la réalité des faits rapportés. Les délais peuvent néanmoins varier en fonction des éléments de l'alerte.

Si une alerte est remontée par un canal différent, l'alerte sera saisie sur la plateforme de signalement et traitée de manière identique.

Le comité d'éthique veille à la confidentialité, à la protection et à la durée de conservation des données personnelles recueillies dans le cadre du traitement de l'alerte.

Le comité d'éthique peut faire appel à des experts internes ou externes dans le cadre du traitement des alertes et, plus généralement, avoir recours aux différents services de Tessi.

DECIDER ET TRAITER L'ALERTE

A l'issue de l'instruction d'une alerte, le pilote propose une date pour réunir le comité d'éthique afin de délibérer sur le dossier concerné. La délibération aura lieu dès lors le comité d'éthique réunit à minima 3 représentants des membres permanents et avec la représentation des bonnes compétences au regard du cas d'alerte concerné.

Le comité d'éthique définira sur la base des faits prouvés les éventuelles sanctions disciplinaires à prendre à l'encontre des individus visés par le signalement ou toute notification éventuelle aux autorités compétentes.

A l'issue du traitement de l'alerte, le lanceur d'alerte sera informé des mesures envisagées ou prises pour le suivi du traitement de son alerte par le comité d'éthique dans un délai d'au plus 3 mois à compter de l'accusé de réception du signalement (ou, à défaut d'accusé de réception, 3 mois à l'issue d'une période de 7 jours ouvrés suivant le signalement).

En cas de potentielle situation de harcèlement moral (article 1152-1 et suivants du code du travail), de harcèlement sexuel (article 1153-1 et suivants du code du travail) ou d'agissement sexiste (article 1142-2-1 du code du travail), l'alerte est transmise pour traitement à la Direction des Droits Sociales.

SUIVI DES ALERTES & SURVEILLANCE DU PROCESSUS

Afin de pouvoir évaluer l'efficacité du dispositif d'alerte et suivre les alertes, le comité d'éthique met en place un suivi annuel statistique concernant la réception, le traitement et les suites données aux alertes.

Ce suivi annuel peut faire apparaître de manière anonyme le nombre d'alertes reçues, de dossiers clos, de dossiers ayant donné ou donnant lieu à une enquête, le nombre et le type de mesures prises pendant et à l'issue de l'enquête (mesures conservatoires, engagement d'une procédure disciplinaire ou judiciaire, sanctions prononcées, etc.).

6. DURÉE DE CONSERVATION DES DONNÉES

- Les données relatives à une alerte considérées comme n'entrant pas dans le champ du dispositif sont détruites sans délai (ou anonymisées).
- Lorsqu'aucune suite n'est donnée à une alerte rentrant dans le champ du dispositif, les données relatives à cette alerte sont détruites ou anonymisées dans un délai de deux (2) mois à compter de la clôture des opérations de vérification. L'expression « suites » désigne toute décision prise par le responsable de traitement pour tirer des conséquences de l'alerte (adoption ou modification des règles internes, réorganisation des opérations ou des services de la société, sanction ou action en justice). Les décisions relatives aux suites réservées aux alertes doivent intervenir dans un délai raisonnable à compter de l'émission de celles-ci.
- Lorsqu'une procédure disciplinaire ou contentieuse est engagée à l'encontre d'une personne mise en cause ou de l'auteur d'une alerte abusive, les données relatives à l'alerte peuvent être conservées par le responsable de traitement jusqu'au terme de la procédure ou de la prescription des recours à l'encontre de la décision.
- À 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 pour assurer la protection de l'auteur de l'alerte ou permettre la constatation des infractions continues. Cette durée de conservation doit être strictement limitée aux finalités poursuivies.

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

7. DESTINATAIRES DES DONNEES ET SOUS-TRAITANTS

Seules les personnes habilitées au titre de leurs missions ou de leurs fonctions peuvent accéder aux données à caractère personnel traitées.

Seuls les référents désignés pour le traitement de chaque alerte accéderont aux données pour le compte des filiales du groupe TESSI afin de recueillir et traiter les signalements émis.

Les alertes reçues peuvent être adressées si nécessaire, aux supérieurs hiérarchiques directs ou indirects de l'auteur de l'alerte et de la personne qui fait l'objet de l'alerte.

Par ailleurs, dans le cadre de son service, la société Valeur & Conformité éditeur de la plateforme de signalement, peut accéder aux données pour réaliser des opérations de maintenance de sa plateforme.

8. INFORMATION DES PERSONNES

L'information des personnes sur le dispositif a été faite dans le cadre des instances représentatives du personnel.

9. DROIT DES PERSONNES CONCERNEES

En fonction de la base légale sur laquelle repose le traitement des données personnelles, les personnes concernées disposent d'un droit d'accès, de rectification, d'effacement, d'opposition et du droit à la limitation du traitement. *« Il est précisé que, conformément à l'article 21 du Règlement général pour la protection des données, 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 de traitement ».*

TESSI garantit à toute personne identifiée dans le cadre du dispositif d'alerte interne le droit d'accéder aux données la concernant et demander leur rectification ou suppression dans l'hypothèse où elles seraient inexactes, incomplètes, équivoques ou périmées. Ce droit s'exerce auprès du DPO du Groupe (dpo.tessi@tessi.fr). La demande devra indiquer le nom et prénom, adresse e-mail ou postale de la personne concernée, être signée et accompagnée d'un justificatif d'identité en cours de validité.

La personne qui fait l'objet d'une alerte ne peut en aucun cas obtenir communication, sur le fondement de son droit d'accès évoqué ci-dessus, des informations concernant l'identité de l'émetteur d'alerte ou d'autres individus.

Le droit d'opposition ne peut être exercé pour les traitements nécessaires à une obligation légale à laquelle est soumis TESSI. De fait, il ne peut s'appliquer aux alertes issues de la loi

Sapin 2 ou du Devoir de vigilance. Il peut être exercé pour les alertes concernant une violation du code éthique de Tessi.

10. MESURES DE SECURITE

Tessi garantit la stricte confidentialité de :

- L'identité de l'auteur d'une alerte,
- L'identité des personnes visées par l'alerte,
- L'identité de tout tiers mentionné dans l'alerte,
- De toutes les informations recueillies dans le cadre du traitement de l'alerte.

Une fois le signalement recueilli, l'échange entre le Référent principal pilote du dossier et l'auteur du signalement se fait via la messagerie de la plateforme signalement.net.

L'absence de recours à cette messagerie ou l'utilisation d'autres moyens de communication n'affecte pas l'éventuelle recevabilité de l'alerte, ni n'expose son auteur à des sanctions.