ENGAGEMENTS RELATIFS AU TRAITEMENT DES DONNEES PERSONNELLES ET AU STATUT DU LANCEUR D'ALERTE A L'ATTENTION DES PERSONNES SOUHAITANT EXERCER UNE ALERTE DANS LE CADRE DU DISPOSITIF D'ALERTE PROFESSIONNELLE

DESPREZ BRAUN Solenne

25/06/2025

qualite@f-initiatives.com

Remonter une amélioration ou non-conformité via GLPI

Principales modifications par rapport à la version précédente		
Version	**Date de validation**	**Titre**
V0	10/09/2020	Création
V1	01/10/2021	Mise sur le nouveau Template Rebranding FI Group
V2	25/06/2025	Màj suite définition lanceur d'alerte et nouveau Template F.initiatives

1 OBJET ET DOMAINE D'APPLICATION

Cette liste permet de connaitre le référent en charge du dispositif du lanceur d'alerte, son éventuel adjoint ainsi que les experts métiers selon l'expertise nécessaire pour mener à bien soit l'étude de la recevabilité de l'alerte soit l'investigation.

2 ARCHITECTURE DOCUMENTAIRE

M:_COMPLIANCE\LANCEUR D'ALERTE

Pour les externes à F.initiatives, cette partie ne vous concerne pas.

3 PROBLEMATIQUE EN TERMES DE DONNEES PERSONNELLES

Le dispositif de lanceur d'alerte permet la collecte et l'analyse d'information relatives à des personnes, les lanceurs d'alerte et les personnes qu'ils désignent. Il constitue donc un traitement de données à caractère personnel susceptible d'exclure l'exercice de certains droits liés aux personnes concernées comme le principe du consentement préalable. Les personnes concernées par un signalement ne seront pas informées dès l'enregistrement de données mettant en cause leur intégrité professionnelle et n'auront pas les moyens de s'y opposer.

4 DEFINITIONS

Bonne foi : La conviction de se trouver dans une situation conforme au droit, avec la conscience d'agir sans léser les droits d'autrui. Le premier élément constitutif de la bonne foi concerne directement l'objet de l'alerte.

Canaux sécurisés : Procédure mise en place au moyen de sécurité informatique dans le but de recueillir des alertes

Comité de gestion des alertes : Comité composé de plusieurs référents « Experts Métiers ».

Confidentialité : La non-divulgation d'éléments de nature à identifier la personne mise en cause par un signalement et celle émettrice de l'alerte. La confidentialité vise à assurer d'une part l'efficacité du dispositif afin que les lanceurs d'alerte puissent agir sans crainte de représailles et, d'autre part, le respect du principe de présomption d'innocence pour la personne visée par l'alerte.

Destinataires des données : Les destinataires sont les personnes habilitées chargées de collecter et traiter les données (Référent, Comité de gestion des alertes, avocats etc.).

Données à caractère personnel : Toute information se rapportant à une personne physique identifiée ou identifiable qui doivent, en principe, en conserver la maîtrise sous réserve des exceptions prévues par la loi.

Lanceur d'alerte : Personne physique collaborateur ou externe (tiers à la société) qui signale ou divulgue, sans contrepartie financière directe et de bonne foi, des informations portant sur un crime, un délit, une menace ou un préjudice pour l'intérêt général, une violation ou une tentative de dissimulation d'une violation d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel

engagement, du droit de l'Union européenne, de la loi ou du règlement. Lorsque les informations n'ont pas été obtenues dans le cadre des activités professionnelles mentionnées au I de l'article 8, le lanceur d'alerte doit en avoir eu personnellement connaissance (Loi du 9 décembre 2016 modifiée par la Loi du 21 mars 2022).

Principe d'indépendance : Le fait d'agir en toute objectivité.

Principe de confidentialité : Le fait de s'assurer que l'information n'est accessible qu'à ceux dont l'accès est autorisé.

Principe de conformité : Le fait d'agir en adéquation avec les objectifs poursuivis.

Principe de neutralité : Le fait d'agir en s'abstenant de prendre parti dans un conflit d'intérêt.

Principe de proportionnalité : Le fait d'agir de manière non excessive au regard des objectifs poursuivis.

Principes déontologiques : Ensemble de principes réunissant les principes de confidentialité, d'indépendance, conformité, proportionnalité, neutralité.

Référent : Personne physique en charge de réceptionner les demandes des lanceurs d'alerte, du déroulement de l'enquête et dont la responsabilité de l'investigation est à sa charge.

Référents « Experts Métiers » : Personnes physiques qui composent le Comité de gestion des alertes, représentant une catégorie de métier différent et siégeant dans chaque service de F.initiatives, afin de pouvoir apporter leur expertise et leur regard au cours de l'investigation. Si l'une des personnes au sein du Comité est visée par l'alerte, le Référent du Comité de gestion des alertes verra avec la direction qui doit siéger au sein du comité à titre exceptionnel, aux fins de remplacer l'Expert Métier en question.

Traitement de données personnelles : Toute opération, ou ensemble d'opérations, portant sur de telles données, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction, etc.) effectuée par F.initiatives, conformément à l'article 4.2 du Règlement Général à la Protection des Données (ci-après « RGPD »).

5 CONTEXTE

Le dispositif est mis en œuvre pour anticiper une exigence légale relative à projet de directive de l'UE **adopté par le Parlement en date du 16 avril 2019**. Sur la base des lois n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre et la loi sapin II du 9 décembre 2016 qui ont créé et détaillé le statut protecteur du lanceur d'alerte en France. Est précisé que F.initiatives ne rentre pas dans les seuils d'applicabilité de la loi Sapin II mais a choisi de s'en inspirer pour mettre en place ses procédures. Le process devra donc être modifié une fois la directive transposée dans la loi française afin de prendre en considération ses spécificités.

Les dispositifs d'alerte professionnelle impliquent nécessairement le recueil et le traitement de données personnelles, à commencer par l'identité du lanceur d'alerte et celle de la personne visée par l'alerte.

La publication par la CNIL du **Référentiel concernant les dispositifs d'alertes professionnelles pour les traitements de données personnelles, le 10 décembre 2019**, a permis d'encadrer le dispositif mis en place au sein de F.initiatives concernant d'une part les lanceurs d'alerte et d'autre part les personnes visées par l'alerte, mais aussi d'intégrer les évolutions liées au RGPD.

6 STATUT DU LANCEUR D'ALERTE

Le lanceur d'alerte bénéficie d'un régime de protection prévu par le Code du travail contre toutes sanction ou mesure de rétorsion susceptible d'être prononcée à son égard. Le code du travail reconnaît au salarié le droit d'alerter immédiatement l'employeur de toute situation de travail dont il a un motif raisonnable de penser qu'elle présente un danger grave ou imminent pour sa vie ou sa santé ainsi que toute défectuosité qu'il constate dans les systèmes de protection. Attention, il appartient à F.initiatives de vérifier que le lanceur d'alerte entre bien dans le champ d'application pour bénéficier de cette protection.

Plusieurs dispositions interdisent ou sanctionnent de nullité le licenciement ou le prononcé d'une sanction ou d'une mesure défavorable à une personne qui témoigne de faits dont elle a connaissance dans l'exercice de ses fonctions en matière de discrimination, de harcèlement sexuel ou moral (*Prendre connaissance de la note F.initiatives « Note à l'attention des salariés relative au traitement de leurs données personnelles dans le cadre de la procédure de signalement de faits de harcèlement sexuel ou d'agissement sexiste »*.) Si votre alerte concerne un acte d'harcèlement sexuel ou d''agissement sexiste, merci de vous tourner vers le référent harcèlement sexuel à l'adresse : referentharcelement@f-initiatives.com.

7 CHAMP D'APPLICATION DU DISPOSITIF D'ALERTE : CONDITIONS LIEES A LA PERSONNE ET A LA RECEVABILITE DE L'ALERTE

Le droit d'alerte est une faculté dont dispose tout citoyen (collaborateur de F.initiatives ou tiers à la société) pour signaler ou révéler une atteinte grave. L'octroi du statut juridique de lanceur d'alerte dépend du **respect des conditions suivantes**, à savoir :

- Une démarche désintéressée (tant sur le plan matériel que moral, que ce soit pour lui ou pour des tiers, l'objectif étant d'écarter ceux qui poursuivent un objectif de vengeance ou un profit personnel) ;
- Avoir eu personnellement connaissance des faits rapportés (cette condition exclut donc tous les faits obtenus par déduction ou supputation. L'auteur du signalement doit avoir une connaissance tangible des faits incriminés. Le signalement porte sur des faits mesurables ou réels de conflit d'intérêts par exemple.)
- Être de bonne foi (c'est-à-dire qu'il doit avoir des motifs raisonnables de croire à la véracité des dysfonctionnements signalés.) En effet, le lanceur d'alerte doit avoir l'intime conviction, que la situation qu'il dénonce est contraire à l'éthique et à la déontologie. Il ne peut donc pas relater des faits que lui seul estime subjectivement injustes, anormaux ou inhabituels. Son appréciation des faits considérés doit être guidée par les lois, les règlements, et les règles déontologiques applicables à l'exercice de ses missions ;
- Ne pas tirer profit ou de rémunération de l'alerte émise (tout signalement ne doit pas être motivé pour son propre compte mais pour défendre l'intérêt général) ;
- Ne pas chercher à nuire (l'alerte ne peut servir de voie d'accès à la dénonciation calomnieuse, l'autopromotion ou l'instrumentalisation.).
- L'abus dans l'exercice du droit de signalement : la dénonciation calomnieuse est punie de 5 ans d'emprisonnement et de 45 000 euros d'amende (Code pénal art. 224-10).

8 CONDITIONS LIEES AUX SIGNALEMENTS OU REVELATIONS

Exclusions du régime de protection : « Les faits, informations ou documents, quel que soit leur forme ou leur support, couverts par le secret de la défense nationale, le secret médical ou le secret des relations entre un avocat et son client » (loi du 9 décembre 2016)

Les conditions liées au signalement : La personne qui souhaite procéder à une alerte doit se conformer à la procédure de signalement élaborée par F.initiatives (*Prendre connaissance du document dit « Engagements et principes relatifs à l'examen interne des remontées des lanceurs d'alerte »*)

- D'abord le lanceur d'alerte doit soit saisir son supérieur hiérarchique soit le Référent
- En l'absence de retour de la personne auprès de laquelle a été porté le signalement elle doit adresser le signalement à l'autorité administrative.

Le dispositif mis en place pour le recueil des signalements doit être « clair, accessible, et sécurisé » selon le décret du 19 avril 2017.

A ce titre, la procédure de signalement diffusée précise clairement les différentes étapes de la procédure :

Les modalités suivant lesquelles le lanceur d'alerte doit (i) adresser son signalement au supérieur hiérarchique direct ou indirect à l'employeur, à l'employé ou à un référent désigné par l'employeur par voie postale ou messagerie sécurisée) (ii) transmettre les informations et documents à l'appui de son signalement (iii) indiquer le moyen de communiquer avec lui.

Les délais de traitement de l'information par l'employeur (i) pour accuser réception après 2 jours ouvrés de l'alerte, (ii) pour examiner l'alerte et indiquer les suites données sur la nécessité d'ouvrir ou non une investigation (7 jours ouvrés).

9 PRINCIPES RELATIFS AU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL DANS LE CADRE DE LA PROCÉDURE DE SIGNALEMENT

Les personnes concernées par ce traitement peuvent être :

- Toute personne interne à la société, collaborant dans le cadre d'un contrat de travail : intérim, stagiaire, alternant, employé en CDD, en CDI ou dirigeant.
- Toute personne tierce à la Société : Prestataires, agents publics, clients, prospects etc.

Conformément à l'article 5 du RGPD, ces données collectées doivent être traitées de manière licite, loyale et transparente à l'égard :

- Du lanceur d'alerte (auteur du signalement) qu'il soit collaborateur ou tiers à la Société.
- De la personne visée par l'alerte.
- De toutes les personnes intervenant dans le recueil ou le traitement de l'alerte incluant les témoins, le référent et les référents « Experts métiers ».

Toutefois, compte tenu du contexte précis, l'autorisation de ces personnes pour ce traitement ou bien l'information de ces personnes est encadrée dans les conditions prévues ci-après.

10 RAPPEL DE LA BASE LEGALE DU TRAITEMENT

L'article 6 du RGPD impose que chaque traitement soit accompagné d'une base légale pour qu'il soit effectivement licite.

A ce titre, le dispositif mis en place est licite puisque :

- L'encadrement du dispositif résulte d'une obligation légale, le traitement est prévu par la Loi Sapin II, et il est **nécessaire à la constatation, à l'exercice ou à la défense de droits en justice.**
- Il participe à la protection de l'intérêt légitime de F.initiatives : Le référentiel de la CNIL anticipe les évolutions introduites par directive européenne du 16 avril 2019 relative à la protection des lanceurs d'alerte dont le texte a été adopté début octobre par le Conseil de l'Union européenne, pour une application effective prévue à partir de 2021 (bien que cette directive ne soit pas encore transposée en droit national, F.initiatives a décidé de s'inspirer des directions de cette directive).
- Le consentement de la personne auteur du signalement est toujours recueilli dans la mesure où cette personne a consenti au traitement de ses données personnelles par un acte positif en se tournant volontairement vers son supérieur hiérarchique ou le Référent. Toutefois, l'auteur du signalement peut ne pas donner pas son consentement sur la révélation de son identité.

  Le consentement de la victime (dans les cas de discrimination) et / ou de la personne visée par la procédure n'est pas nécessaire, compte tenu du fait qu'il s'agit de l'application d'une obligation légale (le traitement étant un moyen prévu par la Loi Avenir Professionnel afin de permettre d'établir si un délit a eu lieu ou non au sens de l'article 222-33 du Code pénal).

11 NATURE DES DONNEES COLLECTEES RESPECTANT LE PRINCIPE DE MINIMISATION CONSIDERANT TOUTES EVENTUALITES DE COLLECTE

Voici les données qui seront collectées dans le cadre d'une alerte et de son traitement.

- **Emetteur de l'alerte** : Son nom, son prénom, (identification de son supérieur hiérarchique à qui l'alerte aurait déjà été remontée et non traitée le cas échéant), données de connexion (adresse IP, logs), téléphone, adresse e-mail

personnelle, adresse e-mail professionnelle. Le lanceur d'alerte choisit délibérément d'utiliser son adresse email personnelle ou professionnelle.

- **Personne visée par l'alerte** : Son identité, les faits qui lui sont reprochés, sa fonction, ses coordonnées.
- **Référent et/ou référent « Expert métiers »** : Son identité, son adresse e-mail professionnelle, les objectifs poursuivis et les domaines concernés par les alertes.
- **Concernant les données traitées du ou des témoins éventuels** : Nom, prénom, fonction, et éventuellement leurs coordonnées et leurs témoignages.
- **Concernant l'alerte** : Recueil des faits signalés, les éléments recueillis dans le cadre de la vérification des faits signalés, le compte rendu des opérations de vérification (poursuite ou non de la procédure), suite donnée à l'alerte.
- **Si l'alerte concerne des faits de discrimination** : La collecte de données sensibles (éventuellement relatives à la santé, à l'orientation sexuelle, aux opinions politiques, aux activités syndicales, etc.).
- En tout état de cause, les données recueillies doivent être strictement limitées à ce qui est nécessaire pour vérifier les faits. A ce titre, ce sera le rôle du Référent de trier dans les données reçues afin de s'assurer qu'elles sont toutes strictement nécessaires dans le cadre de l'alerte.

12 FINALITES DE LA PROCEDURE DE SIGNALEMENT

Le traitement relatif aux personnes concernées concerne une ou plusieurs finalités spécifiques.

Ces finalités, au regard du RGPD doivent être déterminées, explicites et légitimes et ne pas être traitées ultérieurement d'une manière incompatible avec les finalités initiales.

Dans le cadre de la procédure du dispositif mis en place, la finalité principale est celle de la **gestion des signalements recueillis.**

En outre, les sous-finalités initiales du traitement sont :

- Réception et enregistrement des demandes et signalements
- Traitement des alertes émises par un membre du personnel ou un tiers
- Le suivi des demandes et signalements
- L'évaluation de l'alerte et de sa recevabilité
- Le respect de la confidentialité et de la sécurité des données
- Le respect des délais mis en place
- Le cas échéant, mise en œuvre d'une procédure disciplinaire
- Le cas échéant, saisine de l'autorité judiciaire

13 DESTINATAIRES DES DONNÉES PERSONNELLES DANS LE CADRE DE LA PROCÉDURE

Les données collectées dans le cadre de la procédure sont strictement confidentielles. Une adresse email est dédiée au recueil des alertes : lanceurdalerte@f-initiatives.com ou par voie postale.

Les destinataires de l'alerte se limitent aux :

- Référent et/ou suppléant identifié au sein de la société ;
- Experts Métiers désignés au sein du Comité de gestion des alertes ayant un lien avec l'alerte remontée après qu'un tri ait été effectué par le Référent pour s'assurer que seules les informations nécessaires sont transmises ;
- Personnes en charge de l'enquête (avocats, etc.) ;

Dans le cadre du traitement de l'alerte, les personnes habilitées pourront potentiellement être averties dans le cadre de leur mission ou si leur fonction le nécessite :

- Supérieur hiérarchique de l'émetteur de l'alerte (si la fiche de signalement est remise à celui-ci ou dans le cadre d'une procédure disciplinaire) ;
- Service RH : dans le cas où une sanction disciplinaire est décidée à l'encontre de la personne visée par l'alerte et/ou une mesure proportionnelle permettant de sauvegarder les intérêts en jeu est mise en place. Aussi, dans le cas où **le Président de la société est visé par la procédure, en cas de décision de lancer une investigation, le DRH en sera informé ;**
- La Direction Juridique et Fiscale sous réserve que cela soit nécessaire (par exemple, dans le cadre d'éventuelles sanctions disciplinaires) ;
- **Service IT** : en fonction du risque de gravité une traçabilité des adresses IP, un gel des serveurs et conservations des back up / données, extraction et sauvegarde des données par constat d'huissier peut être effectué ;
- Les témoins éventuels (incluant mais sans se limiter au n+1 des personnes concernées) ;
- **L'équipe DPO** : dans le cas d'une demande de droit d'accès ;
- Autorités judiciaires et les représentants de la force publique, en cas d'infractions ou de condamnations pénales.

14 RETRAIT DU CONSENTEMENT : EXERCICE DU DROIT D'ACCÈS AUX DONNÉES PERSONNELLES

Concernant l'information de la personne visée par l'alerte : Dès l'enregistrement des données la concernant, la personne visée par l'alerte doit être informée du traitement de ces données, afin de lui permettre notamment d'exercer ses droits d'accès, d'opposition, de rectification ou de suppression des données. Cette information peut néanmoins intervenir a posteriori, lorsqu'il apparaît nécessaire d'adopter des mesures conservatoires afin de prévenir la destruction de preuves.

Effectivement, par exception, lorsque l'information de la personne visée par l'alerte *« est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement »*, alors cette dernière ne peut en aucun cas avoir connaissance de l'identité du lanceur d'alerte.

Concernant les droits d'accès, de rectification et de suppression : Toutes les personnes identifiées dans le cadre de l'alerte doivent avoir connaissance de l'existence de leurs droits d'accès, de rectification et de suppression des données les concernant, et être en mesure d'exercer ces droits de manière effective. Toutefois, le droit d'accès par la personne concernée ne doit pas présenter un danger dans le déroulement de l'enquête (par ex : la découverte de certaines informations qui pourrait mettre en danger ou compromettre l'enquête.)

Le droit d'accès, de rectification, de suppression est cependant limité à la réserve d'une base légale comme motif.

Compte tenu de l'identification de 3 catégories de personnes dans le cadre du dispositif, il convient de distinguer les droits applicables pour chacun :

- **La personne émettrice de l'alerte (collaboratrice de F.initiatives ou tiers)** : A le droit d'accéder à ses données personnelles ou de rectifier celles-ci en faisant directement la demande à l'adresse dpo@f-initiatives.com ou bien s'il s'agit d'un tiers à la Société sur le site internet de F.initiatives dans l'onglet « exercice du droit d'accès ». Toutefois, le Référent devra s'assurer que les modifications demandées ne sont pas exercées sous pression et pourra choisir de ne pas en tenir compte s'il appert dans l'enquête que les faits remontés sont exacts.
- Par ailleurs, le retrait du consentement n'est pas possible compte tenu du risque trop important que cela résulte de pressions subies. Toute remontée d'alerte devra être traitée selon la procédure et ce jusqu'à la clôture (qu'il y'ait eu investigation ou non.).

- **Les personnes visées par l'alerte (auteurs présumés)** : Ont un droit d'accès restreint, elles pourront obtenir l'accès au dossier et l'accès à leur données personnelles, en faisant directement la demande à F.initiatives par le biais de

l'adresse dpo@f-initiatives.com. Toutefois, celles-ci ne pourront pas avoir accès au nom de la personne ayant émis l'alerte. En tout état de cause, ce droit d'accès pourra uniquement avoir lieu sous réserve de ne pas compromettre l'enquête en cours.

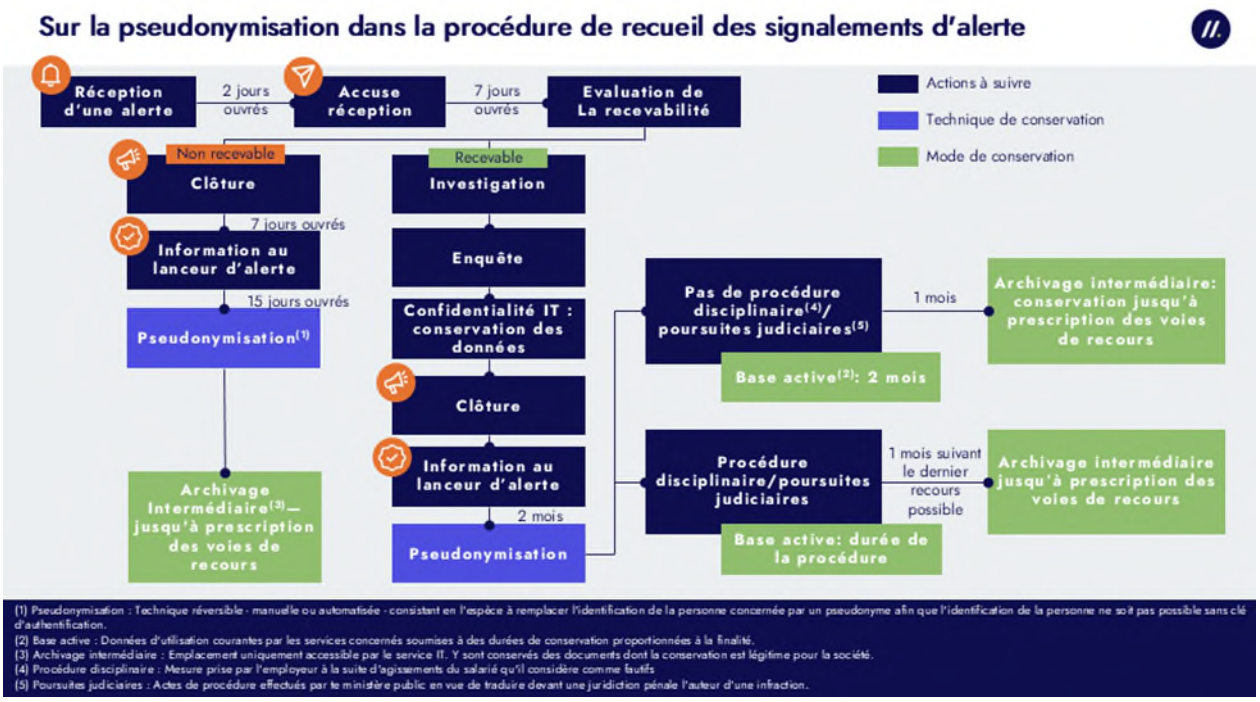
- **Les personnes qui sont victimes / témoins** : Ont le droit d'accéder à leurs données personnelles à l'adresse dpo@f-initiatives.com, ou bien de rectifier celles-ci sous condition de ne pas compromettre l'enquête en cours.

15 OBLIGATIONS DU RGPD RELATIVES AUX LANCEURS D'ALERTE

Les obligations portées par le RGPD s'appliquent à tous les traitements, anciens comme nouveaux, et nécessitent que F.initiatives prennent notamment les mesures suivantes :

- Inscrire le dispositif de recueil des alertes professionnelles dans le registre des traitements.
- Effectuer une analyse d'impact relative à la protection des données.
- Informer les personnes concernées de la mise en place de la procédure.

17 DELAI D'EFFACEMENT



Les données sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard de l'obligation légale ou du consentement de la personne concernée (voir ci-dessus : « retrait du consentement ») ou de l'intérêt légitime de la société).

La durée de conservation des données dépend, d'une part, des données concernées, et, d'autre part, des suites données à l'alerte. La personne référente au sein de l'organisme a la charge de la vérification de la pseudonymisation des données personnelles :

- **Si l'alerte est considérée comme n'entrant pas dans le champ du dispositif dès son recueil :**
  - Dans la base active : pseudonymisation de la demande dans les 15 jours suivants un classement sans suite au sein du recueil et archivage intermédiaire des documents reçus.
  - Dans l'archive intermédiaire : pendant la durée légale de prescription afin que F.initiatives puisse démontrer pourquoi elle a archivé sans suite la demande en cas de contentieux.
- **Si l'alerte n'est pas suivie d'une procédure disciplinaire ou judiciaire :**
  - Dans la base active : 2 mois suivant la clôture de l'investigation ou la décision de ne pas effectuer de procédure disciplinaire ou judiciaire
  - Dans l'archive intermédiaire : le mois suivant la pseudonymisation de la donnée, pendant la durée légale de prescription afin que F.initiatives puisse démontrer pourquoi elle a archivé sans suite la demande en cas de contentieux.

- **Si l'alerte est suivie d'une procédure disciplinaire ou de poursuites judiciaires :**
  - Dans la base active, jusqu'à la prescription des voies de recours de la procédure.
  - Dans l'archive intermédiaire : dans le mois suivant le dernier recours possible.

En tout état de cause, le registre avec les informations pseudonymisées permet de constater les différentes actions entreprises par le Référent. Chaque fichier est chiffré par un mot de passe sur le réseau et le réseau bénéficie d'un cloisonnement des accès.

18 CONFIDENTIALITE / SECURITE

En application de l'article 9 de la Loi SAPIN, l'identité du lanceur d'alerte pourra potentiellement être divulguée aux personnes dont la connaissance de l'identité serait indispensable dans le cadre de la procédure, une fois le caractère fondé de l'alerte établi et après avoir accord écrit exprès du lanceur d'alerte. Est expressément rappelé que le consentement du lanceur d'alerte n'est pas nécessaire pour divulguer son identité à l'autorité judiciaire.

La divulgation de l'identité du lanceur d'alerte est punie de 2 ans d'emprisonnement et de 30 000 euros d'amende (Loi du 9 décembre 2016, art. 9). Les données relatives au lanceur d'alerte et à la personne visée par l'alerte doivent être traitées de manière confidentielle. Enfin, les informations recueillies dans le cadre de l'alerte doivent elles aussi demeurer confidentielles. La divulgation de ces éléments confidentiels est punie de deux ans d'emprisonnement et de 30.000 euros d'amende.

Un canal d'information sécurisé est instauré afin de protéger les parties prenantes contre d'éventuelles menaces ou représailles pour garantir l'effectivité de cette protection.

Le traitement de l'alerte est encadré par la mise en place de :

- Un protocole relatif à la communication sera déterminé et devra être respecté par les Experts Métiers ;
- Une pseudonymisation du fichier puis archivage intermédiaire par le service IT ;
- Un gel des serveurs et conservations des back up / données, extraction et sauvegarde des données par constat d'huissier.

Les données personnelles des personnes concernées sont traitées de façon à garantir une sécurité appropriée, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées.

L'adresse email dédiée au recueil des alertes : lanceurdalerte@f-initiatives.com possède un accès restreint et protégé par un mot de passe. Les informations sont confidentielles, et uniquement destinées à certaines catégories de personnes citées ci-dessus (« les destinataires des données dans le cadre de la procédure »).

Dans le cadre de la sécurité imposée par le dispositif d'alerte professionnel, l'organisme a adopté des mesures appropriées afin de garantir un niveau de sécurité adapté au risque se limitant ici aux mesures qui intéressent le dispositif mis en place :

Catégories	Mesures	Mesures mises en place chez F.initiatives
Sensibiliser les utilisateurs	Informer et sensibiliser les personnes manipulant les données	La présente note d'information ainsi que procédure à destination de l'accueil.
Authentifier les utilisateurs	Définir un identifiant (login) unique à chaque utilisateur	La charte informatique de la Société prévoit que chaque utilisateur dispose d'un identifiant et d'un mot de passe strictement personnels pour leur session. 10 tentatives avant verrouillage. Profils utilisateurs pour tous/administrateurs du poste pour le helpdesk/administrateur du domaine pour les administrateurs système/responsables IT Fait lors des revues des droits d'accès/départ des collaborateurs.
Gérer les habilitations	Profils et permissions	Annuellement revue des droits d'accès logique/applicatif et 2x par an physique. Pour avoir des habilitations pour avoir accès à un dossier ou à un logiciel particulier, les utilisateurs doivent faire la requête au Service Informatique via l'outil ticketing et avec validation de son supérieur hiérarchique.
Tracer les accès et gérer les incidents	Système de journalisation	Système de recensement des logs centralisé sur un serveur. Les informations telles que l'identité des utilisateurs et des appareils, les dates et détails relatifs aux évènements comme l'accès aux données.
Sécurité des postes de travail		La session de chaque utilisateur possède un mot de passe personnalisé qui doit impérativement être modifié à chaque période définie (70 jours). Par ailleurs, la session se verrouille après quinze minutes d'inactivité. Si le technicien informatique désire prendre la main à distance du poste informatique de l'utilisateur, l'utilisateur doit préalablement avoir accepté cette prise en main via « Assistance ».
Sécuriser le réseau informatique interne	-Limiter les flux au strict nécessaire -Sécuriser les accès distants des postes nomades	- Microsoft Office 365 ne peut communiquer avec l'entreprise qu'avec le protocole HTTPS. - Les accès distants des appareils informatiques nomades sont sécurisés par le réseau virtuel sécurisé Citrix ou VPN - Norme ISO 27001 certifiée par Bureau Veritas
Sécuriser les serveurs	Limitez l'accès aux outils et interfaces d'administration aux seules personnes habilitées	L'accès aux outils et interfaces est limité au seul service informatique. Aussi, à l'intérieur même du service informatique, les accès sont limités et sont gérés selon leur niveau d'habilitation. Vérification des updates quotidien, poussés toutes les semaines. L'accès aux systèmes de fichiers NTFS sur le serveur est composé de quatre lecteurs réseau : -Base documentaire (M :) -Clients (V :) -F.initiatives (X :) -Partage (Z :)

		Chaque lecteur réseau possède des accès restreints aux personnes habilitées et sont paramétrés par le service informatiques
Sécuriser les sites web		Le site web F.initiatives utilisent le protocole TLS (assure le chiffrement des données grâce à une clé de cryptage asymétrique, rendant les informations échangées illisibles pour une personne tierce et sécurisant la connexion. Il prouve également l'identité du détenteur du certificat SSL / TLS correspondant.)
Archiver de manière sécurisée	- Mettre en œuvre des modalités d'accès spécifiques aux données archivées - Détruisez les archives obsolètes de manière sécurisée	Les données sont stockées sur un serveur d'archivage Un process d'archivage intermédiaire a été mis en place. Actuellement, l'automatisation de l'archivage sur les dossiers clients est en cours de réalisation.
Contrôle des accès logiques		Pour avoir des habilitations pour avoir accès à un dossier ou à un logiciel particulier, les utilisateurs doivent faire la demande à leurs responsables de service. Ce dernier se chargera de transmettre la requête au Service Informatique. Le contrôle d'accès logique est mis en place par identifiant et mot de passe. Une politique de mot de passe est déployée au sein de la Charte SSI qui mentionne que l'authentification des services est faite au travers d'un unique annuaire spécialisé et maîtrisé sauf exception justifiée. Les utilisateurs ont des identifiants uniques et les mots de passe sont strictement personnels et confidentiels. Ces mots de passe sont changés à intervalles réguliers (70 jours). L'accès aux ressources du réseau est limité aux utilisateurs autorisés sur l'annuaire.
Cloisonnement		Cloisonnement du serveur, grâce aux accès restreints des collaborateurs réservés aux personnes habilitées => Dossier crée dans le but de cloisonner l'accès aux personnes habilitées et par rapport au reste du système d'information
Anonymisation/pseudonymisation		Possibilité pour la personne lançant une alerte de ne pas indiquer les informations permettant de l'identifier (anonymisation). Fichiers pseudonymisés (voir plus haut) avant archivage intermédiaire.
Sauvegarde des données		- Processus de redondance, de sécurité et de sauvegardes garantissant la disponibilité et l'intégrité des données. - Sauvegarde quotidienne de l'ensemble de l'infrastructure et comprenant les sauvegardes des serveurs, des données, des logiciels et application métiers et permet de pallier un défaut logiciel, matériel, d'une attaque externe ou erreur interne.
Sécuriser les locaux	Restreignez les accès aux locaux au moyen de portes verrouillées	Tous les accès des bâtiments de F.initiatives sont sécurisés grâce à des portes verrouillées, ouvrable uniquement grâce à un badge (clé électronique paramétrées par la Société) ainsi que des vidéos de télésurveillance possédant un système de floutage.

Maintenance		L'ensemble des opérations de maintenance et des changements techniques sont enregistrés dans l'outil ticketing.

19 LEGISLATION APPLICABLE

- Article 6 (1) c du règlement européen 2016/679 (Règlement Général sur la Protection des Données - RGPD)
- Le traitement est nécessaire au respect d'une obligation légale à laquelle la CNIL est soumise, en particulier :
  - Loi n°83-634 du 13 juillet 1983 modifiée portant droits et obligations des fonctionnaires, notamment son article 28 bis ;
  - Loi n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique ;
  - Décret n° 2017-564 du 19 avril 2017 relatif aux procédures de recueil des signalements émis par les lanceurs d'alerte au sein des personnes morales de droit public ou de droit privé ou des administrations de l'Etat.