Report2Box by datax

Politique en matière de systèmes d'information internes
Auteur: DATAX
Juin 2023

INDEX

1. Objet, champ d'application et principes directeurs

1.1. OBJET ET FINALITÉ

La présente politique a pour objet d'expliquer à tous les utilisateurs du système d'information interne de l'entreprise (ci-après dénommé "SII" ou "canal de dénonciation") comment il fonctionne, comment ils peuvent y accéder et quelles sont ses fonctionnalités. C'est-à-dire ses principes généraux de fonctionnement ainsi que ceux de la défense du dénonciateur.

Le canal d'alerte est l'outil par lequel tous les membres de l'entreprise, c'est-à-dire les membres de l'organe de direction, les cadres et les employés, ainsi que les tiers qui ont ou ont eu une relation de travail ou professionnelle avec l'entreprise, peuvent informer cette dernière des éventuels risques et violations de ses règles (tant légales qu'internes) dont ils ont connaissance (il s'agit des informateurs ou communicateurs). Ces tiers, c'est-à-dire ceux qui devraient être autorisés à faire un rapport, devraient être au moins les actionnaires, les participants et les membres de l'organe de direction, y compris les membres non exécutifs, les travailleurs indépendants, toute personne travaillant pour des contractants, des sous-traitants et des fournisseurs ou sous leur supervision, les anciens employés, les stagiaires, les candidats à des processus de sélection ou à des négociations précontractuelles, les bénévoles et les stagiaires de l'entreprise.

L'objectif est de créer un mécanisme qui garantisse, entre autres, le respect de la loi et l'efficacité du code d'éthique et des protocoles internes de l'entreprise, en évitant qu'ils ne deviennent de simples déclarations d'intention.

L'utilisation de ce canal peut également permettre à l'entreprise d'adapter son activité à la réglementation en vigueur, de garantir le respect de ses règles internes et de réduire le risque de comportement criminel ou illicite au sein de l'entreprise, protégeant ainsi également ses employés.

1.2. CHAMP D'APPLICATION ET FORCE EXÉCUTOIRE

Champ d'application objectif : ce qui peut et ne peut pas être signalé par l'intermédiaire du SII :
Les communications faites par l'intermédiaire du canal de dénonciation doivent porter sur des actions ou des omissions qui se produisent dans le champ d'action de l'entreprise et qui constituent une violation, dans un contexte professionnel, d'une règle ou d'un principe affectant l'entreprise. Dans tous les cas, elles doivent être signalées :

Comportement constituant une infraction pénale ou une infraction administrative grave ou très grave telle que, par exemple, un délit de fraude, le versement d'une commission indue ou le non-paiement d'une taxe
a) tout acte ou omission du droit de l'Union européenne à condition que :

- Concerne les questions relatives aux marchés publics, aux services, produits et marchés financiers et à la prévention du blanchiment de capitaux et du financement du terrorisme, à la sécurité et à la conformité des produits, à la sécurité des transports, à la protection de l'environnement, à la radioprotection et à la sûreté nucléaire, à la sécurité des denrées alimentaires et des aliments pour animaux, à la santé et au bien-être des animaux, à la santé publique, à la protection des consommateurs, à la protection de la vie privée et des données à caractère personnel et à la sécurité des réseaux et des systèmes d'information.
- Elle affecte les intérêts financiers de l'Union européenne ; ou
- Il a un impact sur le marché intérieur, tel que les infractions aux règles de concurrence de l'UE et les aides d'État.

a) Toute violation des règles, principes et valeurs internes de l'entreprise ;
b) Tout événement susceptible d'entraîner un dilemme éthique ;
c) tout événement susceptible de compromettre la réputation de l'entreprise.

Les incidents non inclus dans cette section, tels que les questions étroitement liées aux ressources humaines ou aux politiques du personnel (par exemple, les congés, la rémunération, les relations entre les employés, les conflits interpersonnels, etc.), les recommandations ou les suggestions non liées aux questions de conformité réglementaire ou à la prestation de services de l'entreprise, ne sont pas considérés comme des incidents à signaler.

En cas de doute sur la nature du fait en question de la part de l'informateur, et à condition que l'informateur agisse de bonne foi, le fait peut être signalé sans problème. L'officier IIS examinera son contenu et analysera son éventuelle recevabilité, qui sera communiquée à l'informateur.

Préoccupations
Si les destinataires de la présente politique ont des préoccupations concernant le respect de la réglementation ou l'utilisation du canal d'alerte (par exemple, comment interpréter une réglementation ou comment agir dans un cas particulier), ils peuvent s'adresser à clima@refrica.com.

Champ d'application subjectif : à qui s'adresse cette politique ?
La présente politique s'adresse aux actionnaires de la société, ainsi qu'à tous ceux qui, d'une manière ou d'une autre, fournissent des services à la société sur la base d'un emploi ou d'une activité professionnelle, c'est-à-dire les participants ou les membres des organes de direction, d'administration ou de surveillance de la société, y compris les membres non exécutifs, les employés et les collaborateurs externes réguliers (comme indiqué à l'article 1.1), ainsi que toute personne susceptible d'agir au nom ou pour le compte de la société et de tiers, sans aucune limitation géographique. La politique s'applique également (i) à toutes ces personnes, qu'elles aient le statut de rapporteur, d'enquêté/plaignant ou de témoin et (ii) à l'organe chargé de recevoir et/ou de traiter les plaintes qui peuvent être reçues par le biais du canal de dénonciation, à savoir le responsable de l'IBS (ci-après, le responsable).

Caractère obligatoire :
Son respect constitue une obligation professionnelle ou contractuelle pour tous (à l'exception des tiers), de sorte que son inobservation peut faire l'objet de sanctions disciplinaires conformément aux dispositions de la réglementation du travail où l'entreprise exerce ses fonctions (par exemple, la convention collective d'application), ainsi que dans le règlement ou le document contractuel correspondant.
Tout destinataire de la présente politique est tenu de signaler tout incident dont il a connaissance par les moyens prévus au chapitre suivant.

1.3. RÉGIME JURIDIQUE

L'organisation, l'utilisation et le fonctionnement du canal d'alerte sont régis par la présente politique, qui est complétée par la procédure de gestion des informations reçues. De même, il convient de respecter toute réglementation qui pourrait être émise par les autorités ou les administrations en relation avec les canaux d'alerte ou d'autres réglementations qui pourraient régir des aspects connexes (par exemple, les lois régissant la protection des données à caractère personnel ou la prévention du blanchiment d'argent et du financement du terrorisme et, de manière significative, toutes celles qui régissent la protection des droits fondamentaux).

1.4. PRINCIPES DIRECTEURS

L'adoption du canal de dénonciation répond à la volonté de l'entreprise d'établir un engagement de tolérance zéro à l'égard de la commission de délits, d'infractions administratives, de la non-conformité aux règlements et du respect de la légalité et des bonnes pratiques.
Conformément à ce qui précède, la procédure de gestion des communications reçues par le canal de dénonciation respectera toujours les principes suivants :

Confidentialité : toutes les informations traitées par le canal d'alerte sont considérées comme confidentielles et sont traitées comme telles ; la confidentialité de l'identité de l'informateur et de tout tiers mentionné dans la communication, ainsi que des actions menées dans le cadre de son traitement, est garantie ; seules les personnes autorisées à le faire y ont accès ;
Indemnisation et interdiction des représailles : les utilisateurs de bonne foi du canal de dénonciation seront protégés par l'entreprise, par les autorités le cas échéant, et ne feront l'objet d'aucune mesure de représailles pour l'utilisation correcte du canal ;
Impartialité : le contrôleur observera et traitera toujours les informations qui lui sont soumises de manière objective et impartiale ; et
Confiance : l'entreprise suscitera la confiance de tous ses membres dans l'utilisation de la chaîne afin de la rendre aussi efficace que possible.

2. Rapport d'incident : Comment faire un rapport d'incident ?

2.1. MOYENS DE NOTIFICATION DES INCIDENTS

Les destinataires de la présente politique peuvent déposer les plaintes mentionnées au point 1.2 ci-dessus par l'intermédiaire du canal de plaintes mis en place par l'entreprise, c'est-à-dire par l'intermédiaire de la plateforme Report2Box by Datax accessible par ce lien : https://refrica.report2box.com/home

Si l'informateur le demande, il peut également soumettre sa communication par le biais d'une rencontre en personne avec la personne responsable dans un délai maximum de 7 jours à compter de sa demande.

Afin de garantir la confidentialité du canal, seules les personnes mentionnées ici auront accès aux rapports présentés et seront responsables de leur gestion et de leur traitement : Le Comité d'éthique, qui recevra immédiatement toutes les plaintes qui peuvent être envoyées par le biais de la plateforme indiquée. Si la plainte est justifiée, elle sera communiquée au Comité d'éthique pour qu'il entame les enquêtes correspondantes. De même, la plateforme Report2Box by Datax sera toujours protégée par un mot de passe qui devra être modifié tous les 3 mois et qui ne sera connu que des personnes mentionnées ici. Ces outils et tout autre outil susceptible d'être utilisé pour le traitement des plaintes comprendront également les mesures techniques et de sécurité nécessaires pour garantir la confidentialité du canal de dénonciation.

Les moyens susmentionnés constituent tous les moyens internes de l'entreprise par lesquels la plainte peut être envoyée, et ce sont eux qui doivent être utilisés en priorité. Toutefois, les dénonciateurs peuvent également adresser leurs plaintes à un organisme externe : l'Autorité indépendante de protection des dénonciateurs (IPA) ou toute autre autorité compétente pour recevoir les plaintes.

Si une personne de l'entreprise qui n'est pas le responsable IIS reçoit une plainte par quelque moyen que ce soit, elle doit immédiatement la transmettre au responsable et garder les informations reçues confidentielles.

2.2. INFORMATIONS DE BASE

Les rapports communiqués par l'intermédiaire du canal de dénonciation doivent contenir les informations minimales suivantes :

- Le fait, le comportement ou l'irrégularité signalés, ainsi que la date à laquelle ils se sont produits. Aucune classification ou évaluation juridique du fait examiné par l'informateur n'est requise, bien que l'informateur doive avoir des motifs raisonnables de croire que le fait rapporté est vrai ;
- La raison pour laquelle l'événement est considéré comme étrange ou irrégulier ;
- L'identité des personnes responsables des faits susmentionnés, si elle est connue (les rapports sur des sujets inconnus mais identifiables peuvent être admis) ;
- Les éléments de preuve qui peuvent être disponibles pour prouver que l'événement ou l'irrégularité a été commis (la fourniture de preuves par la partie déclarante n'est pas obligatoire). En aucun cas, les preuves ne doivent être obtenues en violation des droits fondamentaux ou de manière illégale. En cas de doute, l'informateur doit s'abstenir d'obtenir les preuves sans l'avis de la personne responsable ou du tiers qu'il juge approprié ;
- L'identification du plaignant, bien que les communications anonymes puissent également être acceptées. Dans le cas où un rapport anonyme est reçu par le canal de signalement, les informations reçues seront traitées avec les précautions nécessaires requises pour ce type de communication et sans que cette circonstance n'empêche l'application de la présente politique. Dans ce cas, il est important de garder à l'esprit que la plateforme Report2box by Datax permet une communication constante avec le dénonciateur anonyme par le biais d'un code de suivi fourni par la plateforme. Il est important de garder à l'esprit que, dans le cas où le dénonciateur anonyme perd le code de suivi, il ne lui sera pas possible de le récupérer et, par conséquent, d'accéder au suivi de son rapport.

Toutes ces informations sont demandées sur l'écran d'accueil de Report2Box, et seuls les espaces prévus à cet effet doivent être remplis.

Les utilisateurs peuvent également accéder aux instructions d'utilisation du canal grâce à la vidéo explicative qu'ils trouveront sur ce lien : https://youtu.be/3zh5g7kG15g

Dans tous les cas, l'auteur du signalement est tenu de faire un rapport véridique, sans déformer la vérité, et sans préjudice du fait que les informations transmises sont basées uniquement sur des indications d'une infraction telle que visée à la section 1.2. L'utilisation de mauvaise foi du canal de dénonciation, par exemple en faisant des rapports faux ou non fondés, est interdite et sera sanctionnée par l'entreprise.

2.3. INCOMPATIBILITÉ

Dans le cas où la plainte affecte directement ou indirectement le Responsable, la plateforme Report2Box permet de la confier à un second responsable afin de désigner un remplaçant qui devra assumer les tâches de gestion de la plainte en lieu et place du sujet incompatible.
Lorsque cette situation d'incompatibilité avec le Responsable se produit, le fait qu'il ne s'abstienne pas de ses fonctions, constituera un manquement très grave à la présente Politique avec les sanctions prud'homales ou contractuelles conséquentes qui peuvent être imposées.

3. Défense et obligations du dénonciateur

3.1. DÉFENSE ET OBLIGATIONS DU DÉNONCIATEUR

L'entreprise, par l'intermédiaire du contrôleur, veillera à ce que le dénonciateur soit protégé en toute bonne foi et utilise le canal de dénonciation tel qu'il est défini dans la présente politique, en appliquant les principes d'action suivants :

a) garantir et traiter de manière confidentielle votre identité, l'identité des personnes qui peuvent être mentionnées dans la communication que vous faites et les faits qui y sont énoncés. Cela signifie que seules les personnes autorisées à le faire et identifiées ci-dessus auront accès aux informations relatives au rapport et ne les partageront pas avec d'autres tiers.
b) Garantir l'anonymat dans les cas où la communication est faite de cette manière. En d'autres termes, lorsque le dénonciateur effectue son signalement de manière anonyme, son identité ne sera jamais connue, ce qui est garanti par la plateforme Report2Box, qui est gérée par un tiers extérieur à l'entreprise.
c) Fournir un interprète ou des documents traduits lorsque la personne qui fait le signalement en a besoin pour comprendre l'étendue de ses droits et obligations ainsi que l'utilisation du canal d'alerte.
d) Observer une interdiction absolue des représailles de quelque nature que ce soit, y compris les menaces de représailles et les tentatives de représailles, pour les informations qui pourraient être fournies à l'enquête par le dénonciateur. En d'autres termes, si le dénonciateur reçoit de bonne foi une forme quelconque de représailles pour sa coopération avec l'entreprise, le dénonciateur sera immédiatement sanctionné.

Dans le même temps, le déclarant doit tenir compte des obligations suivantes lors de l'utilisation du canal de dénonciation :
a) a) Agir de bonne foi.
b) Ne pas communiquer des faits qui sont faux ou manifestement contraires à la vérité.
c) Fournir le plus de détails possible sur les faits rapportés et coopérer à l'enquête.
d) Assurer le suivi de la plainte déposée afin d'être informé de son traitement et de pouvoir répondre aux clarifications ou demandes d'information qui pourraient être formulées.

e) Respecter la confidentialité des informations fournies et de l'existence même de la plainte et de la procédure de traitement qui s'ensuit.

De même, l'entreprise doit garantir les droits de la personne dénoncée, tels que le droit à l'honneur, à la présomption d'innocence, à ne pas subir d'enquêtes prospectives, à avoir accès aux faits qui lui sont attribués et à être entendue à ce sujet. Tout cela sera inclus dans la procédure de gestion des informations reçues, qui complète le contenu de cette section.

3.2. GRANDS PRINCIPES DE LA PROCÉDURE DE GESTION DE L'INFORMATION

Lorsque le responsable du SGI reçoit une plainte par l'intermédiaire du canal de dénonciation et, sans préjudice des dispositions de la procédure de gestion des informations reçues, il entame la phase d'enquête interne sur les faits signalés, dont les grands principes directeurs sont les suivants :

a) Elle étudie les faits contenus dans la plainte reçue et procède tout d'abord à une analyse de sa plausibilité. C'est-à-dire qu'elle examinera si les faits rapportés doivent ou non faire l'objet d'une enquête, en décidant d'admettre la plainte ou de la rejeter. Cette décision sera notifiée à l'informateur ;
b) Si la plainte passe le filtre de plausibilité susmentionné, le responsable ouvre une enquête interne au cours de laquelle il prend les mesures d'investigation jugées nécessaires, telles que, par exemple, un entretien avec le plaignant (s'il n'est pas anonyme), avec les témoins et avec le plaignant et/ou l'analyse de toute documentation qui pourrait s'avérer nécessaire.
c) Au cours de l'enquête qu'il mène, il respectera à tout moment les droits et les garanties énoncés dans la présente politique, dans la procédure de gestion des informations reçues et dans le système juridique, tels que la proportionnalité, l'impartialité, l'indépendance et les droits de la défense, la présomption d'innocence, l'honneur et la contradiction des parties concernées par l'enquête.
d) Enfin, avec les faits analysés, il émet un rapport de conclusions dans lequel les faits observés sont évalués et une conclusion est tirée. Le cas échéant, le responsable peut également inclure dans son rapport une proposition d'adoption de mesures visant à améliorer les processus de l'entreprise.
e) Sur la base des conclusions formulées par le responsable dans son rapport, l'entreprise analyse s'il y a lieu d'adopter des mesures disciplinaires ou contractuelles ou d'engager une action en justice..

4. La communication

4.1. COMMUNICATION

Une copie de la présente politique sera fournie, soit par des moyens télématiques (par exemple via l'intranet), soit sur papier, à tous les destinataires, afin qu'ils soient conscients de leurs devoirs, droits et garanties en ce qui concerne l'utilisation du canal de dénonciation. En tout état de cause, un accès facile et continu à la présente politique sera assuré à tous ses destinataires par l'intermédiaire de l'intranet ou du dossier de bienvenue de l'entreprise. Si les destinataires de la présente politique ne parlent pas espagnol,

une traduction dans une langue qu'ils comprennent doit être fournie. La preuve de la diffusion de la présente politique à tous ses utilisateurs sera conservée.

En outre, la présente politique sera publiée sur la page d'accueil du site web de l'entreprise, dans une section distincte et facilement identifiable, afin d'en faciliter l'accès.

4.2. INTERPRÉTATION

En cas de doute sur l'interprétation de la présente politique, les questions seront envoyées au responsable via l'adresse électronique indiquée ci-dessus afin qu'elles puissent être résolues.

4.3. FORMATION ET SENSIBILISATION

De même, l'entreprise fournira à tous ses membres une formation spécifique sur l'utilisation du canal de dénonciation, qui s'appuiera sur la présente politique et qui, en tout état de cause, couvrira les points suivants :

- L'existence d'un canal de dénonciation dans l'entreprise aux fins décrites dans le présent document ;
- Comment utiliser correctement le canal de dénonciation et quelle est sa procédure ;
- les droits et les devoirs des utilisateurs du canal de dénonciation ;
- l'obligation pour les destinataires de la présente politique d'informer l'entreprise de tout fait décrit à la section 1.2.

L'entreprise fournira également une formation spécifique sur la gestion du canal de dénonciation aux personnes chargées de recevoir et de traiter les plaintes, en l'occurrence le responsable de l'IMS.

L'entreprise conservera des preuves de toute formation ou autre activité de formation ou de sensibilisation qui aurait pu être organisée pour tous les utilisateurs du canal de dénonciation.

4.4. ENGAGEMENT DES BÉNÉFICIAIRES DE LA POLITIQUE

Tous les membres de l'entreprise doivent connaître la politique, contribuer activement à son respect et signaler tout manquement dont ils auraient connaissance, ainsi que toute lacune qu'ils pourraient observer dans son contenu ou son développement. L'organe directeur de l'entreprise accordera une attention particulière à ces obligations.

5. HISTORIQUE, ADOPTION, ENTREE EN VIGUEUR ET REFORME DE LA POLITIQUE. ÉVIDENCE

5.1. HISTORIQUE, APPROBATION ET ENTRÉE EN VIGUEUR

Historique :

Le tableau suivant présente les différentes versions du manuel qui ont été produites, ainsi que leur date et les modifications ultérieures que chaque version du document a pu subir :

VERSION	DATE	CHANGEMENTS
1.0	*March 2023*	Version initiale
2.0	A déterminer	

Adoption et entrée en vigueur :

La présente politique est approuvée par le comité d'éthique. La date d'approbation est consignée dans le procès-verbal du comité. C'est à partir de cette date que le document entrera en vigueur dans l'entreprise.

5.2. SUIVI, ADAPTATION CONTINUE ET RÉFORME DES POLITIQUES

Contrôle et adaptation continus :

Le contenu de la politique fera l'objet de révisions périodiques afin de garantir son adaptation continue à la réalité de l'entreprise, aux changements législatifs ou jurisprudentiels, etc. De même, son utilisation fera l'objet d'un suivi et la performance du système de dénonciation pourra être mesurée au moyen d'indicateurs. Tout cela en application du principe d'amélioration continue qui régit les processus de l'entreprise.

Réforme :

Le comité d'éthique peut préformuler la politique de sa propre initiative et/ou sur proposition de tout destinataire de la présente politique.

5.3. CONSERVATION DES PREUVES

Le responsable du traitement assure la conservation de toutes les preuves qui attestent des activités de formation, de contrôle, de supervision et de correction qui ont été réalisées dans l'entreprise conformément aux sections précédentes. Cela se fera en coordination avec les règles de protection des données personnelles correspondantes à chaque domaine d'activité de l'entreprise.

6. PROTECTION DES DONNÉES PERSONNELLES

Afin d'assurer le respect de la législation sur la protection des données personnelles et, en général, d'éviter l'utilisation abusive des informations, l'entreprise garantit, dans les processus de gestion et de traitement du canal de dénonciation qui peut être mis en place, tant à l'égard de l'informateur qu'à l'égard de la partie ou des tiers faisant l'objet de l'enquête, que :

- Seuls le chef du système d'alerte interne, les responsables désignés du traitement des données et le délégué à la protection des données auront accès aux données à caractère personnel obtenues en vertu de la présente politique. Ils doivent les garder confidentielles et ne peuvent les utiliser à des fins qui ne sont pas directement liées aux fonctions de gestion et d'instruction du canal d'alerte. Les données à caractère personnel ne sont pas collectées si elles ne sont pas manifestement pertinentes pour le traitement d'une plainte spécifique ou, si elles sont collectées par accident, elles sont supprimées dans les meilleurs délais. Si les informations reçues contiennent des données relevant de catégories particulières de données, elles sont immédiatement effacées.

- Ce n'est que dans le cas où des mesures préventives ou disciplinaires sont prises à l'encontre d'un destinataire de la présente politique que le directeur des ressources humaines ou l'organe compétent se verra accorder l'accès aux données à caractère personnel. De même, en cas d'adoption de mesures disciplinaires, l'accès sera accordé au chef des services juridiques de l'entité ou de l'organisme.

- Les mesures techniques et organisationnelles nécessaires sont prises pour préserver l'identité et garantir la confidentialité des données relatives aux personnes concernées par les informations fournies, notamment celle de la personne qui a pu porter les faits à la connaissance de l'entreprise, si elle a été identifiée.

- L'identité de l'informateur ne peut être communiquée à l'autorité judiciaire, au ministère public ou à l'autorité administrative compétente que dans le cadre d'une enquête pénale, disciplinaire ou prud'homale.

- Les données à caractère personnel ne sont collectées et conservées, le cas échéant, dans le système de signalement que dans la mesure et pour la durée nécessaires pour décider de l'ouverture d'une enquête ou d'une instruction sur les faits signalés et pour ouvrir une telle enquête ou instruction.

En tout état de cause, à l'issue d'un délai de trois mois à compter de l'introduction des données dans la plateforme Report2Box sans qu'aucune enquête n'ait été ouverte, ces données seront supprimées de ce système de réclamation. Les communications restées sans suite ne peuvent être enregistrées que sous forme anonyme (sans obligation de les bloquer).

- Toutes les entités obligées doivent tenir un registre des informations reçues et des enquêtes internes, dont les données à caractère personnel ne sont conservées que pendant la période nécessaire, et en aucun cas pendant une période supérieure à dix ans.

- L'objectif de la collecte de ces données est de pouvoir enquêter, détecter et corriger d'éventuels cas de non-conformité ou de conduite inappropriée au sein de l'entreprise, notamment en matière de droit pénal et de conformité réglementaire.

- Dans la mesure où les données personnelles obtenues à partir de l'instruction seront incorporées dans les systèmes d'information de l'entreprise afin de gérer le canal d'alerte, les parties intéressées pourront exercer les droits visés aux articles 15 à 22 du Règlement général sur la protection des données (cependant, l'accès à la communication ne sera en aucun cas donné aux sujets concernés). Pour ce faire, une lettre doit être adressée à *REFRIGERACION CASASSAS S.A, Carreterra N-IIa, 47 – 17458 FORNELLS DE LA SELVA (Girona)* indiquant la demande spécifique et accompagnant une photocopie de la pièce d'identité du demandeur.

- Les dispositions de l'art. 32 de la loi 10/2010 du 28 avril de prévention du blanchiment d'argent et du financement du terrorisme lorsque l'exercice des droits affecte une plainte liée à la prévention du blanchiment d'argent et du financement du terrorisme.

- Si vous souhaitez contacter directement le délégué à la protection des données de l'entreprise avec l'intention de formuler une réclamation, une question ou un doute, vous pouvez communiquer par écrit avec vos coordonnées à l'e-mail lopd@refrica.com

- Pour plus d'informations sur notre politique de confidentialité, vous pouvez accéder au lien suivant : https://www.refrica.com/politica-de-privacidad/

ANNEXE I

Définitions

a) **Canal de dénonciation**: outil que l'entreprise met à la disposition de tous ses membres et des tiers pour pouvoir, de manière sécurisée, confidentielle et/ou anonyme, signaler des faits pouvant constituer un délit ou une infraction administrative grave ou très grave. De même, peuvent également être communiqués des faits pouvant impliquer la violation d'une règle interne, un fait pouvant affecter la réputation de l'entreprise ou pouvant poser un dilemme éthique.

b) **Personne signalant, alertant ou communiquant**: personne qui, identifiée ou anonyme, communique à l'entreprise l'un des faits ci-dessus. Il peut s'agir d'un membre de l'entreprise ou d'un tiers. Il faut tenir compte du fait que la loi 2/2023 du 20 février réglementant la protection des personnes qui signalent des infractions réglementaires et la lutte contre la corruption ne protégera que celles qui ont une relation de travail ou professionnelle avec l'entreprise et qui signalent un acte qui constitue un infraction pénale ou administrative grave ou très grave. Ceci est sans préjudice de la protection qui peut être accordée à l'informateur auprès d'autres organismes de réglementation.

c) **Personne signalée:** personne présumée responsable et responsable des événements signalés. Celui-ci bénéficiera également de certains droits qui seront développés dans la Procédure de Gestion des Informations Reçues.

d) **Responsable du Système Interne de Réclamations**: organe individuel ou collégial, désigné par l'organe directeur de l'entreprise, responsable de la gestion et/ou du traitement du Canal des Réclamations et des enquêtes internes ultérieures qui peuvent être menées.

e) **Représailles :** tout acte ou omission interdit par la loi ou qui, directement ou indirectement, implique un traitement défavorable qui place les personnes qui les subissent dans une situation particulièrement désavantageuse par rapport aux autres dans le cadre du travail ou professionnel, uniquement en raison de leur statut d'informateur ou pour avoir fait une divulgation publique. Comme par exemple le licenciement, l'absence de promotion interne, les changements de poste, etc.

ANNEXE II

Réception de la Politique Interne du Système d'Information

La signature de ce document certifie que j'ai reçu, lu et compris la Politique Interne du Système d'Information. S'engager, en même temps, à le respecter et à s'y conformer.

De même, je comprends que si je ne respecte pas son contenu, cette circonstance pourrait entraîner une sanction disciplinaire de la part de l'entreprise.

J'accepte également par la présente d'être au courant des modifications apportées à la Politique, ainsi que de lire les futures révisions qui pourraient être apportées à celle-ci.

DATE:

NOM:

SIGNATURE: