Conditions d'utilisation et politique de confidentialité

Ce canal d'information est mis à disposition afin de respecter la réglementation relative à la protection des personnes signalant des violations du droit de l'Union européenne, conformément à la DIRECTIVE (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 relative à la protection des personnes qui signalent des violations du droit de l'Union.

Il s'agit d'un canal sécurisé et totalement confidentiel. Vous pouvez même communiquer avec nous de manière anonyme. Avant d'effectuer un signalement par ce canal, vous devez lire et accepter les conditions d'utilisation (afin de savoir quels faits peuvent être signalés par cette voie et quels lanceurs d'alerte sont protégés par la réglementation) ainsi que la politique de confidentialité.

Dans ce cas, AEG constitue un groupe d'entreprises dont vous pouvez consulter les membres ici (https://www.aeg.com.es/overlays/electrolux-group). Lors de votre signalement, vous devrez identifier l'entreprise concernée dans le menu déroulant disponible dans l'outil. Les présentes conditions d'utilisation s'appliquent à l'ensemble du groupe.

Il est important de comprendre que cette réglementation vise à protéger le lanceur d'alerte contre d'éventuelles représailles dans le cadre de la relation de travail ou professionnelle au sein de laquelle une infraction aurait été commise par l'organisation, ses employés ou ses dirigeants, dans les domaines indiqués ci-dessous, susceptibles de constituer une infraction pénale ou administrative grave ou très grave, ou portant directement atteinte à l'intérêt général.

Par conséquent, avant de fournir toute information, il est important que vous lisiez et preniez en compte les points suivants :

1.- Quelles informations pouvez-vous communiquer par ce canal ?

- Certaines infractions réglementaires ou informations dans le cadre de la lutte contre la corruption visées à l'annexe de la Directive (UE) 2019/1937 du 23 octobre 2019, notamment en matière de :
    - marchés publics et attribution de concessions ;
    - services, produits et marchés financiers (produits bancaires, de crédit, d'investissement, d'assurance et de réassurance, retraites individuelles ou pensions, services de valeurs mobilières, fonds d'investissement, services de paiement), ainsi que prévention du blanchiment de capitaux et du financement du terrorisme ;
    - exigences de sécurité et de conformité des produits commercialisés sur le marché de l'Union ;
    - sécurité des transports ;
    - protection de l'environnement ;
    - protection contre les radiations et sûreté nucléaire ;
    - sécurité des denrées alimentaires et des aliments pour animaux, santé animale et bien-être animal ;
    - santé publique ;
    - protection des consommateurs ;
    - protection de la vie privée et des données personnelles, ainsi que sécurité des réseaux et systèmes d'information ;
    - infractions fiscales, en matière de concurrence et/ou d'aides publiques ;
    - infractions au reste de l'ordre juridique susceptibles de constituer une infraction pénale ou administrative grave ou très grave, ou portant directement atteinte à l'intérêt général ;
    - harcèlement sous toutes ses formes ;
    - autres (à préciser dans le corps du signalement).

2.- Quelles informations NE pouvez-vous PAS communiquer par ce canal ?

Ce canal est destiné à signaler à l'organisation des infractions qu'elle-même, ses employés ou ses dirigeants auraient pu commettre dans les domaines mentionnés ci-dessus, susceptibles de constituer une infraction pénale ou administrative grave ou très grave, ou portant directement atteinte à l'intérêt général.

Il ne doit PAS être utilisé pour :

- signaler des violations du droit privé régissant les relations entre particuliers sans impact sur le bon fonctionnement des institutions publiques ou privées ;
- déposer des réclamations relatives au service ;
- signaler des conflits interpersonnels concernant le lanceur d'alerte et les personnes visées par la communication (sauf s'ils constituent une infraction pénale ou administrative grave ou très grave) ;
- formuler des revendications salariales, de congés, etc. ;
- diffuser des rumeurs ;
- plus généralement, communiquer des informations relatives à des actions ou omissions ne relevant pas du point 1 ci-dessus.

3.- Qui bénéficie de la protection accordée aux lanceurs d'alerte ?

La protection prévue par la réglementation relative à la protection des personnes signalant des violations du droit de l'Union s'applique aux personnes ayant obtenu des informations sur des infractions dans un contexte professionnel ou de travail, notamment :

- les agents publics et salariés ;
- les travailleurs indépendants ;
- les actionnaires, associés et membres des organes d'administration, de direction ou de surveillance d'une entreprise, y compris les membres non exécutifs ;
- toute personne travaillant pour ou sous la supervision de contractants, sous-traitants et fournisseurs ;
- les représentants légaux des travailleurs dans le cadre de leurs fonctions de conseil et d'assistance au lanceur d'alerte ;
- les personnes physiques qui assistent le lanceur d'alerte dans le cadre de l'organisation où il exerce ses fonctions ;
- les personnes physiques liées au lanceur d'alerte et susceptibles de subir des représailles, comme ses collègues ou membres de sa famille ;
- les personnes morales pour lesquelles il travaille ou avec lesquelles il entretient une relation professionnelle ou dans lesquelles il détient une participation significative.

4.- Les informations fournies doivent être communiquées de bonne foi

La loi ne protège pas les personnes qui fournissent des informations fausses, déformées ou obtenues illicitement.

5.- Responsabilité concernant les données personnelles

La fourniture de données personnelles relève de l'entière responsabilité du lanceur d'alerte, qui doit respecter la réglementation applicable. Il est également responsable de la confidentialité et de la conservation de son identifiant et mot de passe d'accès à l'application.

6.- Possibilité de signalement anonyme

Vous pouvez fournir des informations de manière anonyme. Si vous vous identifiez ou indiquez une adresse, un e-mail ou un lieu sûr pour recevoir des notifications, nous vous enverrons un accusé de réception dans les sept jours calendaires suivant la réception du signalement, sauf si cela risque de compromettre la confidentialité de la communication.

7.- Communication avec le lanceur d'alerte

Que vous vous identifiiez ou non, nous vous recommandons de fournir un moyen de maintenir la communication avec vous ou de vous demander des informations complémentaires afin de pouvoir mener l'enquête et vous informer des actions ou omissions qui vous sont attribuées, ainsi que pour vous permettre d'exercer votre droit d'être entendu à tout moment.

Si vous effectuez un signalement anonyme, l'application vous fournira un lien et un code permettant de consulter l'état de votre communication.

Les faits et/ou comportements pouvant être signalés par ce canal, ainsi que le champ de protection, sont définis dans les présentes conditions d'utilisation. Il est probable que nous devions vous contacter pour demander des précisions ou des compléments d'information :

- si vous vous identifiez, nous le ferons via l'e-mail fourni ;
- si vous restez anonyme, nous communiquerons avec vous via l'application.

Dans ce dernier cas, comme nous ne conservons aucune donnée de contact, vous devrez consulter régulièrement l'application afin de vérifier si vous avez reçu des messages. À défaut, l'enquête pourrait être limitée.

8.- Responsable du système

Le signalement sera reçu par le responsable du système.

Des responsables ont été désignés dans différentes localisations européennes, ainsi qu'un responsable au niveau du Groupe.

Nous préserverons l'identité du lanceur d'alerte. Celle-ci ne pourra jamais faire l'objet du droit d'accès aux données personnelles et ne pourra être communiquée qu'à l'autorité judiciaire, au ministère public ou à l'autorité administrative compétente, en veillant dans tous les cas à empêcher l'accès de tiers à cette identité.

La personne visée par les faits signalés ne sera en aucun cas informée de l'identité du lanceur d'alerte ni, le cas échéant, de l'auteur de la divulgation publique.

Nous préserverons également les informations relatives aux personnes concernées par les faits signalés, afin d'éviter qu'une information apparemment crédible mais manipulée, fausse ou motivée par des raisons non protégées par le droit ne leur porte préjudice.

Dans ces cas, la responsabilité incombe exclusivement au lanceur d'alerte, qui devra en répondre, dégageant ainsi l'entité titulaire ainsi que le gestionnaire du système interne d'information de toute responsabilité.

9.- Accès au système interne d'information

Les accès à notre système interne d'information sont limités :

- au responsable du système et, le cas échéant, à ceux qui le gèrent directement ainsi qu'aux sous-traitants éventuellement désignés ;
- au responsable des ressources humaines dans le cadre de mesures disciplinaires ;
- au responsable des services juridiques de l'entité, uniquement si des mesures légales doivent être prises ;
- au délégué à la protection des données.

10.- Respect des droits des personnes concernées

Nous respecterons dans tous les cas :

- la présomption d'innocence ;

- le droit d'être entendu ;
- l'honneur des personnes faisant l'objet d'une enquête.

En cas d'ouverture d'une enquête, sa durée maximale ne pourra excéder trois mois à compter de la réception du signalement, sauf :

- en cas de complexité particulière nécessitant une prolongation, pouvant aller jusqu'à trois mois supplémentaires ;
- ou dans les cas spécifiques où d'autres délais sont prévus par la loi (par exemple en matière de harcèlement).

11.- Canaux externes

Outre ce canal interne, vous pourrez également utiliser, lorsqu'ils seront créés, les canaux externes de signalement auprès des autorités compétentes, notamment l'Autorité indépendante de protection du lanceur d'alerte et, le cas échéant, les institutions, organes ou organismes de l'Union européenne.

12.- Calcul des délais

Pour le calcul des délais prévus par la réglementation concernant la gestion des informations reçues, les périodes de fermeture de l'entité auprès de laquelle vous effectuez le signalement ne seront pas prises en compte, conformément au calendrier applicable (vacances, jours fériés, jours non ouvrables, etc.).

13.- **Politique de confidentialité :**

INFORMATIONS RELATIVES À LA PROTECTION DES DONNÉES PERSONNELLES	
Responsable du traitement	L'entreprise du **GROUPE AEG** avec laquelle le lanceur d'alerte entretient la relation à l'origine des informations communiquées. Vous pouvez consulter la liste des entreprises, leurs adresses et leurs coordonnées sur https://www.aeg.com.es/overlays/electrolux-group Pour toute question relative au traitement des données personnelles dans le cadre du dispositif d'alerte interne, les personnes concernées peuvent contacter le Délégué à la Protection des Données (Data Protection Officer – DPO) à l'adresse suivante: Simone.vanderVen@aegps.com Le système interne d'information est partagé par l'ensemble des entreprises du groupe.
Finalité et base juridique	Finalité : enregistrement et gestion des communications effectuées via le système interne d'information. Base juridique : respect des obligations légales découlant de la réglementation relative à la protection des personnes signalant des infractions réglementaires et à la lutte contre la corruption, ainsi qu'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique conférée au responsable du traitement.
Décisions automatisées	Nous ne prenons pas de décisions fondées exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques concernant la personne concernée ou l'affectant de manière significative de façon similaire.

Destinataires	Nous communiquerons aux tiers les données nécessaires au traitement du signalement et/ou des procédures disciplinaires, de sanction ou pénales qui pourraient, le cas échéant, être engagées (par exemple à l'entreprise chargée de la gestion du système interne d'information, si celle-ci est externalisée, ou aux autorités, entités ou organismes compétents nécessaires). Cette communication constitue une obligation légale. Les données pourront être communiquées au sein du Groupe d'entreprises à des fins internes liées à la gestion du système interne d'information, sur la base de notre intérêt légitime. Nous pouvons effectuer des transferts internationaux de données si cela est nécessaire à la gestion du signalement (par exemple communication à une autre société du groupe, au lanceur d'alerte ou à l'organisme/autorité compétente, lorsqu'ils sont situés hors de l'Europe). Cette communication sera effectuée sur la base de l'article 49.1 e) du RGPD, aux fins de la défense de la réclamation faisant l'objet du signalement. Nous disposons de clauses contractuelles types signées à cet effet avec nos sièges situés en Chine, aux États-Unis et au Mexique. Nous ne traitons pas de catégories particulières de données, sauf si celles-ci figurent dans les informations fournies par le lanceur d'alerte.
Critères de conservation	Les données personnelles relatives aux communications reçues et aux enquêtes internes réalisées seront conservées pendant la durée nécessaire et proportionnée au respect de la réglementation applicable. Si aucune mesure d'enquête n'est engagée dans un délai de trois mois à compter de la réception de la communication, les données seront supprimées, sauf si leur conservation est nécessaire pour démontrer le bon fonctionnement du système. Les communications qui ne donnent lieu à aucune suite ne seront conservées que sous forme anonymisée, sans que l'obligation de blocage prévue à l'article 32 de la LOPD 3/2018 ne s'applique. En aucun cas les données ne seront conservées pendant une durée supérieure à 10 ans.
Droits	Vous pouvez, lorsque cela est applicable, exercer vos droits d'accès, de rectification, de suppression, d'opposition, de portabilité des données, de limitation du traitement, ainsi que le droit de ne pas faire l'objet de décisions fondées exclusivement sur un traitement automatisé, conformément aux informations complémentaires et détaillées disponibles ici : https://www.aeg.com.es/overlays/data-privacy-statement/ Si la personne concernée par les faits relatés dans la communication exerce son droit d'opposition, il sera présumé, sauf preuve contraire, qu'il existe des motifs légitimes et impérieux justifiant le traitement de ses données personnelles. La personne concernée par les faits relatés ne sera en aucun cas informée de l'identité du lanceur d'alerte ou de la personne ayant procédé à la divulgation publique. Nous préserverons l'identité du lanceur d'alerte. Son identité ne pourra jamais faire l'objet d'un droit d'accès aux données personnelles et ne pourra être communiquée qu'à l'autorité judiciaire, au ministère public ou à l'autorité administrative compétente, en exigeant dans tous les cas que l'accès à cette identité par des tiers soit empêché.

	Les personnes effectuant un signalement par ce canal interne peuvent également le faire via les canaux externes d'information auprès des autorités compétentes (une fois ceux-ci disponibles), notamment auprès de l'Autorité indépendante de protection du lanceur d'alerte et, le cas échéant, auprès des institutions, organes ou organismes de l'Union européenne.
Origine des données	Lorsque les données ne proviennent pas directement de la personne concernée, elles ont été recueillies auprès du lanceur d'alerte ainsi qu'à partir des informations contenues dans le signalement fourni par celui-ci.