Politique du canal interne européen d'information

TEKA

Midea

Approuvé par le conseil d'administration de TEKA INDUSTRIAL, S.A.

Politique du canal interne européen d'information Midea & Teka Europe

1. Introduction et objectif

Teka Industrial, S.A., ses filiales et les entités européennes de la division électroménager de Midea font partie du groupe Midea Group Co. Ltd. (« Midea Group »). Midea Group s'engage à mener ses activités dans toutes les régions avec intégrité et dans le respect de la loi.

Dans la région européenne, un canal d'information interne a été mis en place conformément aux exigences de la loi 2/2023 du 20 février, qui régit la protection des personnes signalant des infractions réglementaires et la lutte contre la corruption, transposant 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 (ci-après dénommée **« la directive** »), ainsi que le règlement (UE) 2016/679 et la loi organique 3/2018 relative à la protection des données à caractère personnel et à la garantie des droits numériques. Le canal interne européen d'information intègre tous les canaux de signalement en Europe et son champ d'application inclut Teka Industrial, S.A., toutes ses filiales en Europe et les entités d'électroménager de Midea en Europe et au Royaume-Uni, comme détaillé **dans l'annexe II.**

L'objectif de cette politique est de fournir un canal de signalement disponible pour l'Union européenne (y compris le Royaume-Uni) (ci-après dénommé « le **canal interne européen d'information** ») et elle est conçue, mise en place et gérée de manière à permettre : i) son utilisation accessible ; ii) la soumission de communications écrites et/ou verbales ; (iii) le respect des garanties de confidentialité et d'anonymat, sauf dans les cas où la divulgation est prévue par une règle nationale ou demandée dans le cadre d'une procédure judiciaire ; (iv) la protection contre les représailles ; (v) la gestion efficace des communications et leur suivi approprié ; vi) l'intégration des différents canaux de signalement en Europe (y compris au Royaume-Uni) et ; (vii) la protection des données à caractère personnel.

Le canal interne européen d'information est destiné aux employés et aux tiers de toutes les entreprises figurant à **l'annexe II** et est géré par Teka Industrial, S.A. d'Espagne avec le soutien du responsable du système (ci-après dénommé « le **responsable du** système

»), sans préjudice de l'application dans chaque entité juridique européenne de la législation nationale respective et de l'autonomie et de l'indépendance des entreprises européennes qui ont mis en place un système de gouvernance local et disposent d'un responsable local du système, comme indiqué à **l'annexe I,** et de l'échange d'informations entre les différents gestionnaires du système, le cas échéant, qui sera admissible pour la bonne coordination et la meilleure exécution de leurs fonctions.

Le Conseil d'administration, en tant que responsable de la mise en œuvre et compétent pour la désignation de la personne physique chargée de la gestion du système, a nommé le responsable du service juridique et de la conformité de MIB Midea EU & Teka EU, et comme suppléant, le spécialiste principal de la conformité de MIB Midea EU & Teka EU. Le responsable du système a délégué au responsable local du système en Europe la gestion des communications reçues par le biais du canal interne européen d'information (conformément à **l'annexe I,** qui est mise à jour régulièrement).

L'objectif de cette politique est d'expliquer la procédure interne de gestion du canal européen de signalement, la protection du lanceur d'alerte et l'application des principes généraux d'action, sans préjudice des modifications ou adaptations nécessaires pour se conformer à la réglementation locale applicable aux entreprises en Europe.

En cas de conflit entre la réglementation locale et les principes de la présente politique, la réglementation locale applicable dans chaque cas particulier prévaudra toujours.

2. Qui peut signaler un problème via le canal interne européen d'information ?

Les personnes qui détiennent ou ont obtenu des informations sur des infractions dans un contexte professionnel ou de travail dans l'Union européenne (ci-après dénommées « les lanceurs d'alerte ») peuvent déposer des signalements via le canal interne européen d'information, notamment :

- Les employés.
- Les lanceurs d'alerte qui communiquent ou divulguent des informations sur des infractions obtenues dans le cadre d'une relation de travail ou statutaire déjà

terminée : bénévoles, stagiaires, travailleurs en stage, qu'ils soient rémunérés ou non, ainsi que ceux dont la relation de travail n'a pas encore commencé, lorsque les informations sur les infractions ont été obtenues au cours du processus de sélection ou de la négociation précontractuelle.

- Actionnaires, participants et personnes appartenant à l'organe d'administration, de direction ou de surveillance des entreprises du groupe européen, y compris les membres non exécutifs.

- Les tiers avec lesquels les entreprises entretiennent des relations commerciales, qu'il s'agisse de clients, de fournisseurs, d'agents, de distributeurs, de travailleurs indépendants, de contractants, de sous-traitants — et ceux qui travaillent sous la supervision de ces derniers — ou de fonctionnaires.

3. Comment accéder au canal interne européen d'information ?

En Europe, un canal de signalement est disponible sans préjudice des canaux de signalement locaux (**annexe I**), à l'adresse suivante :

- **Plateforme web : https://whistleblowersoftware.com/secure/MideaEurope**

  Cette plateforme permet d'effectuer des communications par écrit ou verbalement. Les communications peuvent être anonymes, si le lanceur d'alerte le souhaite, et dans n'importe quelle langue, la confidentialité de toutes les communications étant garantie. De même, la plateforme web permet d'indiquer l'entreprise sur laquelle le lanceur d'alerte souhaite faire un signalement.

- **Rencontre** avec le responsable du système dans un délai maximum de 7 jours à compter de la demande, en garantissant la confidentialité.

En outre, dans les entités de plus de 50 employés, **des canaux de signalement locaux** sont mis à la disposition du lanceur **d'alerte**, comme indiqué dans **l'annexe I**.

Sans préjudice du fait que le lanceur d'alerte peut choisir le moyen de communication qu'il préfère, le canal interne européen d'information garantit l'autonomie, la

confidentialité, l'indépendance et l'absence de conflits d'intérêts en raison de son déconnexion avec les activités commerciales et les employés locaux, car sa gestion relève de la fonction de conformité européenne.

Conformément à la réglementation locale applicable, il peut également exister **des canaux de signalement externes** auprès des autorités compétentes et, le cas échéant, auprès des institutions, organes ou organismes de l'Union européenne (ci-après dénommés **« Autorité indépendante de protection des lanceurs d'alerte »** ou « AIPL »). Le lanceur d'alerte sera informé par le responsable du système des canaux de communication externes et des conditions d'accès qui peuvent être mises en place dans les différents pays.

4. Que puis-je communiquer via le canal interne européen d'information ?

Le canal interne européen d'information permet de communiquer tout :

i) **Violation des réglementations externes** : ces communications peuvent inclure des actes contraires à la loi : fraude, corruption, harcèlement, divulgation d'informations confidentielles, dommages aux systèmes informatiques, violation de la vie privée et des données personnelles, droits de propriété intellectuelle, dommages à l'environnement, violations des droits de l'homme ou du travail, etc.

ii) **Non-respect des réglementations internes du groupe Midea** : ces communications peuvent inclure des actes contraires au **code de conduite professionnelle de** Midea ou aux autres politiques et procédures **internes du groupe** Midea.

iii) **Doutes ou questions** liés à l'interprétation des politiques du groupe ou à des questions d'éthique ou de conduite.

5. Quelle est la portée de la protection du lanceur d'alerte selon la directive ?

Les mesures de protection du lanceur d'alerte, établies au paragraphe 8, s'appliquent au lanceur d'alerte et, le cas échéant, aux représentants légaux des travailleurs dans l'exercice de leurs fonctions de conseil et de soutien au lanceur d'alerte, ainsi qu'aux : a) personnes physiques qui, dans le cadre de l'organisation au sein de laquelle le lanceur d'alerte fournit ses services, collaborent au processus ; b) aux personnes physiques liées au lanceur d'alerte et susceptibles de subir des représailles, telles que des collègues de travail ou des membres de la famille ; c) aux personnes morales pour lesquelles le lanceur d'alerte travaille ou avec lesquelles il entretient une relation de travail ou une participation significative.

Les infractions soumises à la protection du lanceur d'alerte seront celles établies par chaque pays au moment de la transposition de la directive, en distinguant entre :

5.1 Champ d'application de la protection de l'Union européenne :

- **les actes ou omissions susceptibles de constituer des infractions au droit de l'Union européenne,** à condition qu'ils i) relèvent du champ d'application énuméré à l'annexe de la directive 2019/1937 du 23 octobre 2019 ; ii) affectent les intérêts de l'Union européenne au sens de l'article 325 du traité sur le fonctionnement de l'Union européenne ; ou iii) ont une incidence sur le marché intérieur au sens de l'article 26, paragraphe 2, du traité sur le fonctionnement de l'Union européenne, y compris les infractions en matière de concurrence et les aides d'État, ainsi que les infractions aux règles ou pratiques fiscales des entreprises visant à obtenir un avantage fiscal qui fausse l'objet ou l'économie de la législation applicable à l'impôt sur les sociétés.

5.2 Champ d'application de la protection espagnole :

- Actions ou omissions pouvant constituer une **infraction pénale**.
- Actions ou omissions susceptibles de constituer une **infraction administrative** grave ou très grave.

5.3 Champ d'application de la protection locale :

Comme indiqué, la réglementation locale de chaque pays européen peut prévoir, au moment de la transposition de la directive, d'autres infractions pouvant être soumises à la protection du lanceur d'alerte.

6. Gestion du canal interne européen d'information

i. Le canal interne européen d'information permet de communiquer par **écrit**, **verbalement** ou par les deux moyens. Les informations peuvent être présentées par écrit, via la plateforme web et par courrier électronique, ou par téléphone via les canaux habilités et détaillés dans la section 3 ci-dessus. À la demande du lanceur d'alerte, elles peuvent également être présentées lors d'une réunion avec le responsable du système dans un délai de sept (7) jours à compter de la demande.

ii. **Les communications verbales** seront documentées, avec le consentement du lanceur d'alerte : i) par un enregistrement ou ii) une transcription complète et fidèle de la conversation, et il lui sera donné la possibilité de vérifier, de rectifier et d'accepter la transcription par sa signature.

iii. Le canal interne européen d'information offre la possibilité de soumettre des communications **anonymes** via la plateforme web.

iv. Lors de l'envoi d'une communication, le lanceur d'alerte peut indiquer une adresse, une adresse électronique ou un lieu sûr afin de recevoir **des notifications** sur l'état de sa communication ou de y renoncer.

v. L'envoi d'une communication via le canal interne européen d'information donnera lieu à la réception d'un **accusé de réception** dans un délai maximum de sept (7) jours calendaires, confirmant la réception de la communication, sauf si cela peut compromettre la confidentialité de celle-ci.

vi. Le responsable du système informera le lanceur d'alerte, la personne concernée et les témoins du traitement de leurs données dans les termes prévus par la directive.

vii. Lorsque la communication est envoyée via le site web, un **numéro d'accès et un mot de passe** seront générés à la demande du lanceur d'alerte, grâce auxquels il pourra suivre sa communication.

viii. Le responsable du système informera le dénonciateur du résultat de l'enquête dans un délai ne dépassant **pas trois (3) mois** à compter de la réception de la communication ou trois (3) mois à compter de l'expiration du délai de sept jours après la réalisation de la communication, sauf dans les cas particulièrement complexes nécessitant une prolongation du délai, auquel cas celui-ci pourra être prolongé jusqu'à un maximum de trois (3) mois supplémentaires.

ix. Le responsable du système peut **communiquer** avec le lanceur d'alerte et lui demander des informations supplémentaires.

x. De même, le responsable du système pourra compter sur le **soutien et la collaboration d'autres services** du groupe ou de l'entreprise ou de conseillers externes, si nécessaire, dans le cadre de l'enquête.

xi. La communication à **la personne concernée** de la plainte relative aux actes ou omissions qui lui sont reprochés, ainsi que de son droit d'être entendue, aura lieu au moment et de la manière que le responsable du canal interne européen d'information jugera opportuns pour garantir le bon déroulement de l'enquête.

xii. Le droit à la **présomption d'innocence et à l'honneur** des personnes concernées par la communication sera respecté.

xiii. De même, les personnes concernées bénéficieront de la même protection que celle prévue pour les lanceurs d'alerte, leur identité étant préservée et la confidentialité des faits et la protection des données à caractère personnel étant garanties.

xiv. Si les faits communiqués relèvent du domaine de compétence du responsable du système ou sont susceptibles de créer un **conflit d'intérêts** pour l'une des personnes impliquées dans le processus de gestion et/ou d'enquête de la communication, la personne concernée s'abstiendra d'intervenir dans le processus de traitement de celle-ci.

xv. Le responsable du système peut **refuser l'admission** lorsque les faits communiqués, entre autres, manquent de crédibilité et de fondement.

xvi. Le système de gestion du canal interne européen d'information est conçu et mis en place pour **une gestion sécurisée** et conforme à la réglementation en matière de protection des données.

xvii. Le canal interne européen d'information garantit la **confidentialité** de l'identité du lanceur d'alerte et de tout tiers mentionné dans la communication, **en empêchant l'accès à tout personnel non autorisé**. En aucun cas, l'accès à la communication présentée par le lanceur d'alerte ne sera accordé, sauf si l' , l'autorité judiciaire, le ministère public ou l'autorité administrative compétente l'exigent dans le cadre d'une enquête pénale, disciplinaire ou sanctionnatoire.

xviii. Le responsable du système dispose d'une **procédure pour gérer les communications reçues** via le canal interne européen d'information qui complète la présente politique.

7. Absence de représailles

Le Groupe veillera à ce qu'aucun acte constituant des représailles, y compris les menaces de représailles et les tentatives de représailles, ne soit exercé à l'encontre des personnes qui soumettent une communication via le Canal interne européen d'information.

On entend par représailles tout acte ou omission qui, directement ou indirectement, implique un traitement défavorable plaçant les personnes qui en sont victimes dans une situation particulièrement désavantageuse par rapport à d'autres dans le contexte professionnel ou de travail, uniquement en raison de leur statut de lanceurs d'alerte ou du fait qu'elles ont fait une divulgation publique, à condition que ces actes ou omissions aient lieu pendant la procédure d'enquête ou dans les deux ans suivant la fin de l'enquête.

À titre d'exemple, sont considérées comme des représailles celles qui, en raison de leur qualité de lanceurs d'alerte, prennent la forme :

- Suspension du contrat de travail, licenciement, résiliation de la relation de travail ou statutaire, y compris le non-renouvellement ou la résiliation anticipée d'un contrat de travail temporaire après la période d'essai, ou la résiliation anticipée ou l'annulation de contrats de biens ou de services, l'imposition de toute mesure disciplinaire, la rétrogradation ou le refus de promotion et toute autre modification substantielle des conditions de travail ; la non-conversion d'un contrat de travail temporaire en contrat à durée indéterminée, lorsque le travailleur avait une attente

légitime d'être proposé pour un emploi permanent ; sauf si ces mesures sont prises dans le cadre de l'exercice régulier du pouvoir de direction prévu par la législation du travail ou la réglementation applicable aux fonctionnaires, en raison de circonstances, de faits ou d'infractions avérés, et sans rel tion avec la présentation de la communication au Canal interne européen d'information.

- Dommages et préjudices, y compris les atteintes à la réputation, les pertes économiques, la coercition, l'intimidation, le harcèlement ou l'ostracisme.
- Évaluation ou références négatives sur les performances professionnelles ou de travail uniquement en raison de leur statut de lanceurs d'alerte.
- Inscription sur des listes noires ou diffusion d'informations dans un certain secteur, rendant difficile ou impossible l'accès à l'emploi ou la passation de marchés de travaux ou de services.
- Refus ou annulation d'une licence ou d'un permis.
- Refus de formation.
- Discrimination ou traitement défavorable ou injuste.

Si le Groupe a connaissance de représailles en cours ou passées, il prendra les mesures raisonnables pour y mettre fin et y remédier. Ces mesures peuvent, selon le cas, consister à :

- Réintégrer la personne dans le même poste ou dans un poste équivalent, avec le même salaire, les mêmes responsabilités, le même titre et la même réputation ;
- Permettre un accès équitable à la défense, à la formation, aux opportunités, aux avantages et aux droits.
- Rétablir la personne dans son ancien poste au sein de l'organisation ;
- Mettre fin ou retirer tout conflit ou litige pouvant exister à l'encontre de la personne (par exemple, l'attitude ou le traitement réservé) ;
- Présenter des excuses pour tout préjudice subi ;

8. Mesures de protection auprès de l'Autorité indépendante pour la protection des lanceurs d'alerte.

Les lanceurs d'alerte qui signalent des violations des sections 5.1, 5.2 et 5.3 ont droit à des mesures de protection auprès de l'Autorité indépendante pour la protection des lanceurs d'alerte (ci-après **« AAI »)** que chaque pays européen a mise en place, le cas échéant, lorsque les circonstances suivantes sont réunies :

- Il existe des motifs raisonnables de croire que les informations en question sont véridiques au moment de leur communication, même si aucune preuve concluante n'est fournie, et que ces informations relèvent du champ d'application des paragraphes 5.1, 5.2 et 5.3.
- La communication ou la divulgation a été effectuée conformément aux exigences de la directive ou d'autres réglementations locales applicables.

Les personnes qui communiquent ou divulguent :

i. Les informations contenues dans des communications qui ont été jugées irrecevables.
ii. Des informations liées à des plaintes concernant des conflits interpersonnels ou qui ne concernent que le lanceur d'alerte et les personnes visées par la communication ou la divulgation.
iii. Des informations qui sont déjà dans le domaine public ou qui ne constituent que de simples rumeurs.
iv. Les informations faisant référence à des actions ou omissions qui ne relèvent pas du champ d'application des sections 5.1, 5.2 et 5.3 de la présente politique.

Tout cela, sans préjudice des conditions et exclusions supplémentaires qui peuvent être prévues par d'autres réglementations locales applicables.

Les mesures de soutien de l'Autorité indépendante pour la protection des lanceurs d'alerte, en fonction de la réglementation de chaque pays, peuvent consister, selon le cas, à fournir :

i. Des informations et des conseils exhaustifs, indépendants et gratuits sur les procédures et les recours disponibles, la protection contre les représailles et les droits de la personne concernée.

ii. Une assistance efficace pour la protection contre les représailles.
iii. Une assistance juridique dans les procédures pénales et civiles transfrontalières, conformément à la législation et à la réglementation communautaire applicable.
iv. Un soutien financier et psychologique, à titre exceptionnel, après évaluation par l'AAI de chaque pays.

Tout cela sans préjudice du droit à l'aide juridictionnelle gratuite pour la représentation et la défense dans les procédures judiciaires, qui pourrait également être accordée en vertu de la réglementation de chaque pays.

Le responsable du système fournira au lanceur d'alerte des informations sur les mesures de soutien proposées par les autorités nationales compétentes.

9. Protection des données et confidentialité

Le traitement des données à caractère personnel du canal interne européen d'information sera effectué conformément aux exigences fixées dans le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/ CE (ci-après dénommé **« RGPD »),** ainsi que la loi organique 3/2018 du 5 décembre relative à la protection des données à caractère personnel et à la garantie des droits numériques (ci-après dénommée **« LOPDGDD »)**. À cet effet, TEKA INDUSTRIAL S.A., titulaire du numéro d'identification fiscale A-39004932 et dont le siège social est situé Calle Cajo 17, 39011 Santander, Espagne, est l'entité responsable du traitement.

9.1. Limitation de la finalité

Les données à caractère personnel collectées par le biais du canal interne européen d'information seront traitées dans le seul but de traiter les communications reçues et d'enquêter sur les faits signalés.

9.2. Légitimité du traitement

Le traitement des données à caractère personnel, dans le but de traiter les communications reçues par le biais du canal interne européen d'information, est licite et trouve son fondement juridique dans le respect d'une obligation légale, conformément aux dispositions de l'article 30.2 de la loi 2/2023.

Le traitement des données non obligatoires, ainsi que le traitement des données à caractère personnel résultant d'une divulgation publique, sera fondé sur l'intérêt public prévu par le RGPD, conformément aux dispositions de l'article 6.1.e) du RGPD.

Le traitement de catégories particulières de données à caractère personnel pour des raisons d'intérêt public essentiel peut être effectué conformément à l'article 9.2.g) du RGPD.

9.3. Limitation de l'accès aux données :

L'accès aux données à caractère personnel contenues dans le canal interne européen d'information sera limité : i) au responsable du système et à la personne qui gère directement les canaux locaux de signalement ; ii) au service des ressources humaines, lorsqu'il convient de prendre des mesures disciplinaires ; iii) au bureau d'éthique du groupe, lorsqu'il est nécessaire de l'impliquer dans l'enquête et/ou qu'il convient de prendre des mesures juridiques ou disciplinaires ; iv) les sous-traitants, et v) le délégué à la protection des données, si cela est obligatoire, et vi) toute autre personne qui doit y accéder pour des raisons dûment justifiées.

En outre, les données à caractère personnel peuvent être partagées avec d'autres entités du groupe Midea afin de coordonner, gérer et, le cas échéant, mettre en œuvre les actions et/ou mesures nécessaires à la gestion et au traitement de la communication et, le cas échéant, à l'enquête ouverte dans chaque cas.

Les données à caractère personnel (y compris les catégories particulières de données à caractère personnel) peuvent être transférées et stockées dans un pays de destination situé en dehors de l'Espace économique européen (« EEE »). Elles peuvent également être traitées par la société mère et les filiales en dehors de l'EEE. Lorsque l'entreprise transfère des données à caractère personnel en dehors de l'EEE, elle veille à ce que toutes les garanties nécessaires soient mises en œuvre pour protéger les données à

caractère personnel de la même manière qu'elles le sont au sein de l'EEE et à ce que le transfert soit conforme au règlement général sur la protection des données et à toutes les autres réglementations applicables. Cela peut être réalisé de plusieurs manières, notamment :

- Le pays de destination vers lequel les données sont envoyées pourrait être approuvé par la Commission européenne pour offrir un niveau de protection adéquat ; ou
- Le destinataire a conclu un contrat basé sur les « clauses contractuelles types » approuvées par la Commission européenne, qui l'obligent à protéger vos données personnelles de la même manière qu'elles sont protégées au sein de l'EEE.

Dans d'autres circonstances, la loi peut autoriser le transfert des données personnelles de l'employé en dehors de l'EEE d'une autre manière. Toutefois, dans tous les cas, l'entreprise veillera à ce que tout transfert de données personnelles soit conforme à la législation en matière de protection des données.

Pour plus de détails sur la protection offerte aux données à caractère personnel lorsqu'elles sont transférées en dehors de l'EEE, vous pouvez contacter dataprotection@teka.com

La communication des données est couverte par l'intérêt légitime de l'entreprise qui consiste à traiter correctement les communications formulées, conformément au considérant 48 du RGPD. Uniquement en cas de détection d'un acte illicite, les données à caractère personnel peuvent être communiquées à des tiers (tribunaux et cours, forces et corps de sécurité ou administration publique), afin de se conformer aux obligations légales correspondantes.

9.4 Durée de conservation des données

Les données traitées dans le Canal interne européen d'information ne peuvent être conservées dans celui-ci que pendant le temps nécessaire pour décider de l'opportunité d'ouvrir une enquête interne.

Dans tous les cas, trois mois après la réception de la communication, elles seront supprimées, sauf si la finalité de leur conservation est de laisser une trace du fonctionnement du canal ou si elles peuvent constituer un délit, auquel cas les informations seront conservées pendant la durée nécessaire à la procédure judiciaire.

9.5. Exercice des droits

Les personnes dont les données à caractère personnel sont traitées dans le cadre et le contexte du canal interne européen d'information seront informées du traitement de leurs données à caractère personnel, dans les conditions prévues aux articles 13 et 14 du RGPD.

Ces dernières peuvent exercer leurs droits d'accès, de rectification, de suppression, d'opposition, de limitation et de portabilité reconnus dans les articles 15 à 22 du RGPD, en écrivant à l'adresse électronique suivante :dataprotection@teka.com ou auprès de l'Agence espagnole de protection des données (www.aepd.es). Toutefois, lorsque la personne concernée exerce son droit d'opposition, il sera présumé, sauf preuve contraire, qu'il existe des motifs légitimes impérieux justifiant le traitement de ses données à caractère personnel, de sorte que ce droit ne sera pas effectif.

Le droit d'accès aux données à caractère personnel ne couvre en aucun cas l'identité du dénonciateur, la possibilité de communiquer cette identité étant limitée uniquement à l'autorité judiciaire, au ministère public ou à l'autorité administrative compétente dans le cadre d'une enquête pénale, disciplinaire ou sanctionnatoire.

9.6. Principe de proportionnalité et de minimisation des données

Seules les données à caractère personnel pertinentes seront collectées. Si leur pertinence pour le traitement d'informations spécifiques n'est pas démontrée ou si elles sont collectées par accident, elles seront supprimées sans délai injustifié. De même, toutes les données à caractère personnel qui ont été communiquées et qui se réfèrent à

des comportements ne relevant pas du champ d'application de la présente politique seront supprimées. Si les informations reçues contiennent des données à caractère personnel relevant de catégories particulières, elles seront immédiatement supprimées, sans être enregistrées ni traitées.

9.7 Mesures de sécurité :

Le canal interne européen d'information est conçu, mis en place et géré de manière sécurisée, de manière à garantir la confidentialité de l'identité du lanceur d'alerte et de tout tiers mentionné dans la communication, ainsi que des actions menées dans le cadre de la gestion et du traitement de celle-ci, en empêchant l'accès à tout personnel non autorisé.

Ainsi, le Canal interne européen d'information dispose de mesures techniques et organisationnelles visant à préserver la sécurité des données collectées et la confidentialité des communications, afin de les protéger contre toute divulgation et tout accès non autorisés.

10. Utilisation du canal interne européen d'information et de la politique

L'utilisation du canal interne européen d'information et de la politique qui le développe se fera de bonne foi, et ne sera pas considérée comme conforme au principe de bonne foi ni à l'objectif de la politique et de la réglementation applicable qui développe la protection des personnes qui signalent des infractions réglementaires et anticorruption, la présentation d'informations fausses, non fondées, déformées, ainsi que celles qui ont été obtenues illégalement dans le but de nuire et de porter préjudice à des personnes ou à toute entreprise de son groupe.

11. Non-respect

Toutes les personnes couvertes par la présente politique sont tenues de se conformer à son contenu. En cas d'identification d'une violation grave de la présente politique ou de tout autre élément du canal interne européen d'information, celle-ci peut et doit être portée à la connaissance du responsable du système.

12. Modifications

La présente politique sera révisée et mise à jour chaque année, sauf si cela s'avère nécessaire à une date antérieure, sans préjudice du fait que le responsable du système puisse apporter les corrections, rectifications ou clarifications nécessaires.

La présente politique remplace toute politique de dénonciation antérieure approuvée par le conseil d'administration de Teka Industrial, S.A.

13. Nature juridique

La présente politique est conforme 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 et du Conseil, et aux exigences de la loi 2/2023 relative à la protection des personnes qui signalent des violations réglementaires et anticorruption.

Tout cela sans préjudice des autres réglementations européennes transposant cette directive, qui seront respectées et applicables à des fins de gestion et de protection si elles ne sont pas expressément prévues dans la présente politique.

Annexe I - Canal local de dénonciation

Zepa SpA	mippolito@carnelutti.com
Midea Italia S.r.l	https://mis.integrityline.com/
Teka Portugal SA	Speak-up@teka.pt

Annexe II : Entités relevant du champ d'application de la présente politique

Teka Industrial, S.A.
Steelgran Components, S.A
Sitre telecom, S.A
Küppersbusch Hausgeräte GMBH
Teka Austria GmbH

Politique du canal interne européen d'information Midea & Teka Europe

Teka CZ SRO
Teka Bulgarie EOOD
Teka Polska Sp Zo.o
SC Teka Küchentechnik Romania Srl
Teka France SAS
Teka Portugal SA
Teka Hellas AE
Zepa SpA
Intra Holding AS
Intra AS
Intra Mölntrop AB
Juvel AS
Midea Europe GmbH
Midea Electric France SAS
Midea Italia Srl
Midea Homeappliances UK Ltd