POLITIQUE DE CONFIDENTIALITÉ (Art. 13-14 GDPR)

Le présent document contient les informations requises par les articles 13 et 14 du règlement (UE) n° 679/2016 (GDPR), en ce qui concerne le traitement des données à caractère personnel des personnes concernées qui sont impliquées, pour diverses raisons, dans des rapports sur des violations pertinentes dans le cadre de la procédure d'alerte du groupe Mastrotto.

Contrôleur

Le contrôleur du traitement des données est

- RINO MASTROTTO GROUP SPA, dont le siège social est situé à Via Dell'Artigianato, 100 – 36070 Trissino (VI) - ITALIE
- NUOVA OSBA SRL, dont le siège social est situé à Via Dell'Artigianato, 100 – 36070 Trissino (VI) - ITALIA
- TESSITURA ORESTE MARIANI SPA, dont le siège social est situé à Via Alfredo Catalani, 75 - 20833 Giussano (MB) - ITALIE
- MORELLINO SRL, dont le siège social est situé à Via Caduti sul Lavoro, 1/3 - 56029 Santa Croce sull'Arno (PI) - ITALIE
- ELMO SWEDEN AB, dont le siège social est situé à Kyrkogatan 18, 512 50 Svenljunga - SUÈDE
- BERMAS MARACANAU INDUSTRIA E COMERCIO DE COURO LTDA, dont le siège social est situé à Av. Sen. Virgílio Távora, S/N - Distrito Industrial I, Maracanaú - CE, 61939-160 - BRÉSIL
- RMG LEATHER USA LLC, dont le siège social est situé à 1226 Fed Ex Drive SW, CONOVER, NC (Caroline du Nord), Zip Code: 28613 – ETATS-UNIS
- BRUSAROSCO DE MEXICO SA, dont le siège social est situé à Industria Zapatera 168, Fracciones de Santa Lucia, 37490 León, Gto. - MEXIKO.

(en particulier, chaque entreprise est le contrôleur des données pour les rapports de violations concernant son organisation).
Le délégué à la protection des données désigné par RINO MASTROTTO GROUP SPA (Avv. Gianluigi Muscas) est domicilié et peut être contacté à l'entreprise.

Contrôle conjoint

Les rapports reçus seront gérés via un service centralisé en mode saas fourni par RINO MASTROTTO SPA, également pour le compte des autres filiales du groupe Mastrotto. Ce service implique le traitement de données partagées entre les filiales et RINO MASTROTTO GROUP SPA, avec l'application d'un régime de contrôle conjoint entre elles conformément à l'art. 26 du RGPD. Pour plus de détails sur les modalités de l'accord de contrôle conjoint, consultez la Procédure d'Alerte du Groupe, consultable sur le site www.rinomastrottogroup.com, rubrique Whistleblowing.

Données personnelles et contribution facultative

En principe, le système d'alerte peut être utilisé **sans que vous ayez à fournir de données personnelles vous concernant** ou concernant des tiers. Toutefois, dans le cadre de la procédure de signalement, vous pouvez **volontairement** divulguer des données personnelles, en particulier des informations sur votre identité, vos nom et prénom, votre pays de résidence, votre numéro de téléphone ou votre adresse électronique.
En règle générale, nous **ne demandons ni ne traitons aucune catégorie particulière de données à caractère personnel**, par exemple sur l'origine raciale et/ou ethnique, les convictions religieuses et/ou philosophiques, l'appartenance à un syndicat ou l'orientation ou la vie sexuelle. Toutefois, grâce aux champs de texte libre du formulaire d'inscription, vous pouvez divulguer volontairement ces catégories particulières de données à caractère personnel si vous le jugez nécessaire.
Le rapport peut également contenir des **données à caractère personnel de tiers**.

Les personnes auxquelles se réfèrent les données personnelles traitées sont i) les personnes au courant des faits signalés, ou qui sont en tout cas invitées à fournir des informations à la suite d'un signalement ii) les "sujets impliqués" (c'est-à-dire accusés de l'infraction objet du signalement), iii) les "sujets protégés" (c'est-à-dire qui bénéficient des protections obligatoires prévues par la législation sur les lanceurs d'alerte par rapport à un signalement), iv) les personnes physiques chargées de cas, v) les autres personnes qui, pour diverses raisons, peuvent être informées de l'existence et suivre-haut du rapport.

Les données traitées peuvent inclure des données et des omissions punissables par un tribunal ou une autorité administrative, notamment également en cas de suspicion de commission d'infractions, de

condamnations pénales ou de mesures préventives conformément à l'art. 10 du RGPD. Ces données conformément à l'art. 10 du RGPD ne doivent être traitées qu'en cas de nécessité absolue, sont documentées par écrit et conservées uniquement dans la mesure strictement nécessaire après que la décision sur l'infraction est devenue définitive dans une procédure dans laquelle elles ont été traitées ; le stockage a lieu, si possible, sans retraitement.

La communication de vos données personnelles est **facultative** et, par conséquent, le fait de ne pas les fournir n'affectera pas votre droit à recevoir un retour d'information après l'envoi de votre rapport et, si vous avez révélé votre identité, à bénéficier des protections prévues par la loi.

Les signaleurs qui traitent les données personnelles dont ils ont connaissance au-delà de ce qui est nécessaire pour donner suite au signalement, assument le rôle de contrôleurs de données conformément à l'art. 4 n 7 du RGPD.

Divulgation de données à caractère personnel

Le responsable du traitement, tout en respectant la **confidentialité de l'**identité du déclarant, peut **partager les** données, conformément aux principes de stricte nécessité, de proportionnalité et de minimisation, avec

i. **d'autres fonctions internes du titulaire**, **que** les gestionnaires de dossiers du **titulaire** jugent approprié d'impliquer dans l'enquête sur un rapport.
ii. **Le gestionnaire de cas, c'est-à-dire** les organes, internes ou externes, désignés par l'entreprise destinataire pour admettre et/ou examiner le rapport sur le fond et/ou pour prendre les mesures qui s'imposent, y compris le retour d'information au déclarant.
iii. **Des tiers expressément désignés en tant que** sous-traitants **externes aux** fins de l'hébergement, de la maintenance ou de la gestion technique du centre de données et de la plateforme en ligne que vous utilisez pour effectuer le rapport et la base de données correspondante.
iv. **Les autorités externes compétentes conformément aux** réglementations applicables (par exemple, les autorités judiciaires, les organes de police, la police financière, l'ANAC - Autorité nationale de lutte contre la corruption, etc.)
v. **Les cabinets d'avocats et/ou les conseillers juridiques, les consultants en matière de conformité des entreprises et/ou les autres personnes impliquées dans le processus d'évaluation du rapport** (par exemple, les témoins experts, les consultants techniques, les autres sociétés de notre groupe au sein desquelles l'enquête et la prise de décision concernant les rapports sont centralisées ou qui sont impliquées d'une manière ou d'une autre dans une violation signalée).

Réalisation technique et sécurité de vos données

Le canal de signalement en ligne comprend une option de communication anonyme via une connexion cryptée. Lors de l'utilisation du système de signalement des infractions, l'adresse IP et la géolocalisation de l'appareil que vous utilisez (PC, tablette, smartphone) ne sont à aucun moment stockées. Nous vous recommandons, dans la mesure du possible, de **ne pas vous connecter au système de signalement à partir d'un appareil de l'entreprise**. Lorsque vous soumettez votre rapport, vous devez créer un mot de passe pour accéder à une boîte de réception sécurisée, afin de pouvoir communiquer avec nous de manière protégée. Il **est de votre devoir de protéger de manière adéquate la confidentialité du code d'identification de votre rapport (qui vous sera communiqué par notre système) et du mot de passe d'accès à la boîte de réception sécurisée**. Nous prenons les mesures techniques et organisationnelles appropriées pour assurer la protection et la confidentialité des données. Le canal de communication Internet utilisé est crypté à l'aide de protocoles avancés. Les données seront stockées dans un format crypté dans un centre de données certifié ISO 27001 situé en Allemagne ou en Suisse.

Les données personnelles non nécessaires à la gestion d'un Signalement ne seront pas collectées ou seront immédiatement supprimées si elles sont collectées de manière non intentionnelle.

Le traitement des données à caractère personnel est licite dans la mesure où il est conforme à un intérêt public aux fins de prévenir ou de sanctionner les infractions à la loi et, dans ce cadre, d'informer et de vérifier sa validité.

Aux fins décrites ci-dessus, les lanceurs d'alerte peuvent procéder à des traitements de données à caractère personnel, en ce qui concerne les données nécessaires à leur signalement.

Transfert de données extra-EEE

Tout transfert de données vers des pays situés en dehors de la zone EEE sera limité à l'utilisation d'un service cloud de productivité individuelle basé sur des centres de données situés aux États-Unis (par exemple Microsoft Office 365) et sera garanti par i) la stipulation, entre notre société et le fournisseur tiers, de clauses contractuelles standard conformément au modèle approuvé par la Commission de l'UE et/ou ii) les dispositions de la convention bilatérale stipulée entre l'UE et les États-Unis appelée "Protection des données transatlantiques". En cas de transfert de données entre notre société et le fournisseur tiers, des clauses contractuelles standard conformes au modèle approuvé par la Commission européenne et/ou ii) aux dispositions de la convention bilatérale conclue entre l'UE et les États-Unis appelée "Trans-Atlantic Data Protection Framework" et/ou une décision d'adéquation de la Commission européenne concernant la législation des États-Unis en matière de protection de la vie privée (à compter de son entrée en vigueur). Dans le cas d'un transfert de données vers la Suisse, la garantie du transfert est la décision d'adéquation de la Commission européenne concernant les lois suisses sur la protection de la vie privée.

Les données peuvent être transférées aux filiales qui sont les contrôleurs de données (ou à d'autres sujets autorisés par eux), basés aux États-Unis, au Brésil et au Mexique, par la société RINO MASTROTTO GROUP SPA, en tant que responsable du traitement des données effectué pour le compte des Responsables de traitement eux-mêmes sur la base d'un contrat de délégation de services de gestion centralisée du cycle de vie des signalements de violations relatifs à ces Responsables de traitement, en mettant à disposition l'accès aux mêmes données. via le service saas Integrity Line.
Dans ce cas, le transfert est limité, de temps à autre, aux données concernant les rapports relatifs à la seule filiale, et est assisté par la garantie constituée par la stipulation, entre les parties, de clauses contractuelles types conformes au modèle approuvé par la Commission européenne.

Les données **ne seront pas diffusées**, sauf dans les cas spécifiquement prévus par le droit national ou le droit de l'Union européenne.

Objectif et base juridique

Les données seront traitées aux fins suivantes : i) évaluer l'admissibilité et le bien-fondé de la dénonciation que vous avez communiquée; ii) appliquer des mesures pour protéger et soutenir les personnes protégées par la législation sur la dénonciation ; iii) assurer le suivi du rapport et, si possible, prendre des mesures pour répondre aux conclusions d'un rapport; iv) appliquer des mesures disciplinaires à l'encontre du dénonciateur qui a signalé l'infraction dans l'intention de nuire ou par négligence grave, ou à l'encontre de toute personne impliquée responsable de l'infraction signalée, v) utiliser les résultats des rapports comme preuve dans les procédures judiciaires.

La base juridique du traitement aux fins visées aux points i), ii) et iii) (en ce qui concerne la mise en œuvre des mesures de réponse aux résultats d'un signalement, strictement nécessaires pour éliminer les conséquences de la violation signalée) est la nécessité de remplir les obligations prévues par la loi, par un règlement ou par une autre législation pour le responsable du traitement.
En ce qui concerne les finalités de mise en œuvre de mesures de réponse aux résultats d'un signalement, éventuellement différentes de celles strictement nécessaires pour supprimer les conséquences de la Violation signalée, la base juridique est l'intérêt légitime du Responsable du traitement à améliorer la structure organisationnelle.
En ce qui concerne les finalités disciplinaires, la base juridique est l'intérêt légitime du Responsable de traitement à poursuivre tout non-respect de la Procédure d'alerte du Responsable de traitement et/ou, plus généralement, de la législation relative à l'alerte.
En ce qui concerne les finalités d'utilisation des données comme preuve dans le cadre d'une procédure judiciaire, la base juridique est l'intérêt légitime du responsable du traitement à exercer la défense de ses droits.

Durée de conservation

Les données personnelles reçues par le contrôleur mais qui ne sont pas strictement nécessaires à l'évaluation du rapport seront immédiatement supprimées.
Les données du rapport et la documentation y afférente seront conservées aussi longtemps que nécessaire pour le traitement du rapport et, en tout état de cause, au plus tard 5 (cinq) ans (en Italie), ou 2 (deux) ans (en Suède) à compter de la date de communication du résultat final de la procédure de

rapport (sous réserve des obligations de confidentialité des informations ainsi que de la limitation du stockage, comme le prévoient les réglementations applicables) et au-delà de ce délai, pendant tout le temps nécessaire à l'accomplissement d'une procédure administrative ou judiciaire déjà engagée ou d'une procédure d'instruction en application du code de procédure pénale. Passé ce délai, les données seront supprimées.

Droits de l'homme

La personne déclarante peut contacter le contrôleur à tout moment, sans aucune formalité, pour exercer les droits suivants : a) accéder aux données, b) rectifier les données si elles sont inexactes, c) mettre à jour les données si elles sont obsolètes, d) demander la suppression des données, e) demander la limitation du traitement des données, f) s'opposer à tout moment au traitement des données pour des raisons découlant de sa situation particulière, g) recevoir notification d'une violation de données dans le cas où celle-ci comporte un risque élevé pour les droits ou libertés fondamentaux des parties intéressées, h) (si le lanceur d'alerte a révélé son identité, ou, dans le cas d'un signalement anonyme, cela est possible même sans révéler son identité) vérifier, corriger et approuver le texte d'un rapport qui a été transcrit par le responsable du traitement après être reçu sous une forme qui ne nécessite pas l'utilisation d'une forme écrite (par exemple, lors d'une rencontre personnelle, d'un appel téléphonique ou d'une autre forme orale non enregistrée, courrier ordinaire). Le retrait du consentement n'affecte pas la licéité du traitement et de la communication effectués sur une base volontaire jusqu'au retrait.

Après avoir demandé une preuve de votre identité (sauf si vous avez décidé de rester anonyme), nous accuserons réception de votre demande d'exercice de vos droits dans les 30 jours suivant la réception du rapport, sauf si une enquête spéciale est nécessaire, auquel cas nous vous enverrons un avis.

Tant que et dans la mesure où il est nécessaire de protéger l'identité d'un lanceur d'alerte, d'un autre sujet protégé tel que défini par la législation en vigueur, ou de personnes intéressées par une action de suivi (par exemple, les gestionnaires de cas, les personnes informées des faits signalés), et pour atteindre les finalités de prévention et de répression des Contrefaçons, notamment pour empêcher les tentatives d'empêcher, d'altérer ou de retarder les Informations ou les actions ultérieures fondées sur les Informations, notamment pendant la durée d'une procédure administrative ou judiciaire ou d'une procédure préliminaire en vertu de du Code de procédure pénale, les droits suivants d'une personne physique concernée ne s'appliquent pas:
- Droit à l'information, Droit de rectification, Droit à l'effacement, Droit à la limitation du traitement, Droit d'opposition, Droit à la notification d'une violation de données personnelles.
Par conséquent, en cas de survenance des conditions ci-dessus, le contrôleur du traitement s'abstiendra de fournir des informations à une personne concernée par un Rapport.

Si le dénonciateur estime que les droits susmentionnés ont été violés, il peut toujours déposer une plainte auprès de l'autorité de contrôle compétente.

En Italie, l'Autorité de contrôle est le Garante per la protezione dei dati personali, dont les bureaux se trouvent à Piazza Venezia, 11 - 00187 Rome, PEC : protocollo@pec.gpdp.it.

En Suède, l'Autorité de contrôle compétente est Integritetsskyddsmyndigheten (YMY) - FE 7744 - 831 90 Östersund - Suède.
Téléphone : +46 (0)8 657 61 00 ; Courriel : imy@imy.se ; Adresse postale: Integritetsskyddsmyndigheten, Box 8114, 104 20 Stockholm, Suède.