INTEGRITETS POLICY (artikel 13-14 i GDPR)

Detta dokument innehåller den information som krävs enligt artiklarna 13 och 14 i EU-förordning 679/2016 (GDPR), i samband med behandling av personuppgifter om registrerade som av olika anledningar är inblandade i att rapportera betydande överträdelser enligt Whistleblowing-förfarandet av Mastrottogruppen.

Ägare

Ägare av behandlingen av personuppgifter är:

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

(särskilt varje företag är personuppgiftsansvarig för uppgifter som rör rapporter om överträdelser som rör dess organisation).

Dataskyddsombudet utsett av RINO MASTROTTO GROUP SPA (Avv. Gianluigi Muscas) har sin hemvist och kan kontaktas på företaget.

Samägande

De mottagna rapporterna kommer att hanteras genom en centraliserad tjänst i saas-läge och tillhandahålls av RINO MASTROTTO GROUP SPA, även på uppdrag av de andra dotterbolagen i Mastrootto Group. Denna tjänst innefattar behandling av data som delas mellan dotterbolagen och RINO MASTROTTO GROUP SPA, med tillämpning av ett gemensamt kontrollsystem mellan dem i enlighet med art. 26 i GDPR. För mer information om villkoren för samägandeavtalet, se Group Whistleblowing Procedure, som kan ses på webbplatsen www.rinomastrottogroup.com, Whistleblowing-sektionen.

Personuppgifter och frivilliga bidrag

I princip kan visselblåsarsystemet användas **utan att du lämnar några personuppgifter om** dig själv eller tredje part. Som en del av rapporteringsförfarandet kan du dock **frivilligt lämna ut** personuppgifter, särskilt information om din identitet, namn och efternamn, bosättningsland, telefonnummer eller e-postadress.
I regel **begär eller behandlar vi inte några särskilda kategorier av personuppgifter, t.ex.** om ras och/eller etniskt ursprung, religiös och/eller filosofisk övertygelse, medlemskap i fackförening eller sexuell läggning eller liv. På grund av fritextfälten i registreringsformuläret kan du dock frivilligt lämna sådana särskilda kategorier av personuppgifter om du anser att det är nödvändigt.
Rapporten kan också innehålla **personuppgifter från tredje part**.

De personer som de behandlade personuppgifterna avser är i) personer med kännedom om de fakta som rapporterats, eller som i vart fall uppmanas att lämna information efter en anmälan ii) "inblandade föremål" (d.v.s. anklagade för överträdelseobjektet i anmälan), iii) "skyddade subjekt" (dvs. som åtnjuter det obligatoriska skydd som föreskrivs i whistleblowingslagstiftningen i förhållande till en anmälan), iv) Case Manager fysiska personer, v) andra personer som av olika anledningar kan göras medvetna om existensen och följer upp av rapporten.

De uppgifter som behandlas kan omfatta uppgifter och försummelser som är straffbara av domstol eller förvaltningsmyndighet, särskilt även vid misstanke om brott, och om brottsdomar eller förebyggande åtgärder enligt art. 10 i GDPR. Sådana uppgifter enligt art. 10 i GDPR ska behandlas endast vid absolut nödvändighet, dokumenteras skriftligen och förvaras endast i den utsträckning som är strikt nödvändig efter att beslutet om brottet har vunnit laga kraft i ett förfarande där de behandlades; lagring sker om möjligt utan upparbetning.

Det är frivilligt att **lämna** dina personuppgifter och om du inte gör det påverkar det inte din rätt att få feedback efter att du har skickat din rapport och, om du har avslöjat din identitet, att åtnjuta det skydd som lagen ger.

Rapportörer som behandlar personuppgifter av sina kunskaper utöver vad som är nödvändigt för att följa upp rapporten, övertar rollen som personuppgiftsansvariga enligt art. 4 n 7 i GDPR.

Utlämnande av personuppgifter

Den personuppgiftsansvarige får, med respekt för **sekretessen för rapportörens** identitet, **dela** uppgifterna, i enlighet med principen om strikt nödvändighet, proportionalitet och minimering, med

i. **Andra interna funktioner hos Innehavaren**, **som Innehavarens handläggare** anser lämpliga att involvera i utredningen av en rapport.
ii. **Case Manager, dvs.** de organ, interna eller externa, som utsetts av det mottagande företaget för att ta emot och/eller granska rapporten i sak och/eller vidta följdåtgärder, inklusive återkoppling till rapportören.
iii. **Tredje parter som uttryckligen utsetts till externa** personuppgiftsbiträden i syfte att tillhandahålla hosting, underhåll eller teknisk hantering av datacentret och den onlineplattform som du använder för att utföra rapporteringen och den relaterade databasen.
iv. **Behöriga externa myndigheter enligt** tillämpliga bestämmelser (t.ex. rättsliga myndigheter, polismyndigheter, finanspolisen, ANAC - den nationella antikorruptionsmyndigheten, etc.).
v. **Advokatbyråer och/eller juridiska rådgivare, compliance-konsulter och/eller andra som är involverade i processen att bedöma rapporten** (t.ex. expertvittnen, tekniska rådgivare, andra företag i vår koncern där utredning och beslutsfattande av rapporter är centraliserat eller som på något sätt är involverade i en rapporterad överträdelse).

Teknisk realisering och säkerhet för dina uppgifter

Online-rapporteringskanalen innehåller ett alternativ för anonym kommunikation via en krypterad anslutning. När du använder rapporteringssystemet för brott lagras inte IP-adressen och geolokaliseringen för den enhet du använder (PC, surfplatta, smartphone) vid någon tidpunkt. Vi rekommenderar att du, om möjligt, **inte ansluter till rapporteringssystemet från en företagsenhet**. När du skickar in din rapport måste du skapa ett lösenord för att få tillgång till en säker inkorg, så att du sedan kan kommunicera med oss på ett skyddat sätt. **Det är din skyldighet att på lämpligt sätt skydda sekretessen för både identifieringskoden för din rapport (som kommer att meddelas dig av vårt system) och lösenordet för åtkomst till den säkra inkorgen**. Vi vidtar lämpliga tekniska och organisatoriska åtgärder för att säkerställa dataskydd och sekretess. Den internetkommunikationskanal som används är krypterad med hjälp av avancerade protokoll. Uppgifterna lagras i ett krypterat format i ett ISO 27001-certifierat datacenter i Tyskland eller Schweiz.

Personuppgifter som inte är nödvändiga för hanteringen av en rapport kommer inte att samlas in eller kommer att raderas omedelbart om de samlas in oavsiktligt.

Behandlingen av personuppgifter är laglig i den mån den överensstämmer med ett allmänt intresse i syfte att förebygga eller bestraffa lagöverträdelser, och i detta sammanhang att lämna information och verifiera dess giltighet.
För de ändamål som beskrivs ovan kan meddelararna utföra behandlingen av personuppgifter, vad gäller de uppgifter som krävs för deras rapportering.

Extra-EES dataöverföring

Eventuella dataöverföringar till länder utanför EES-området kommer att begränsas till användningen av en molntjänst för individuell produktivitet baserad på datacenter i USA (t.ex. Microsoft Office 365) och kommer att garanteras genom i) fastställandet, mellan vårt företag och tredjepartsleverantören, av standardavtalsklausuler i enlighet med den modell som godkänts av EU-kommissionen och/eller ii) bestämmelserna i den bilaterala konvention som fastställts mellan EU och USA kallad "Trans-Atlantic Data Protection". vårt företag och tredjepartsleverantören, standardavtalsklausuler i enlighet med den modell som godkänts av EU-kommissionen och/eller ii) bestämmelserna i den bilaterala konvention som ingåtts mellan EU och USA kallad "Trans-Atlantic Data Protection Framework" och/eller ett beslut om adekvat skyddsnivå från EU-kommissionen om USA:s integritetslagstiftning (från och med dess ikraftträdande). När det gäller överföring av uppgifter till Schweiz är garantin för överföringen EU-kommissionens beslut om adekvat skyddsnivå för schweiziska lagar om integritetsskydd.

De uppgifterna kan överföras till dotterbolagen som är personuppgiftsansvariga (eller till andra personer som är auktoriserade av dem), baserade i U.S.A., i Brasilien och i Mexiko, av företaget RINO MASTROTTO GROUP SPA, som chef för utförd databehandling på uppdrag av de personuppgiftsansvariga själva på grundval av ett kontrakt för tilldelning av centraliserade förvaltningstjänster för livscykeln för rapporter om överträdelser som hänför sig till dessa datakontrollanter, genom att göra tillgång till samma data tillgänglig. genom saas Integrity Line-tjänst. I detta fall är överföringen från tid till annan begränsad till uppgifterna om rapporter som hänför sig till det enstaka dotterbolaget och biträds av garantin som utgörs av kravet mellan parterna av standardavtalsklausuler som överensstämmer med den modell som godkänts av EU-kommissionen.

Uppgifterna kommer inte att **spridas,** utom i de fall som särskilt anges i nationell lagstiftning eller i Europeiska unionens lagstiftning.

Syfte och rättslig grund

Uppgifterna kommer att behandlas i syfte att i) bedöma tillåtligheten och fördelarna med den visselblåsarrapport som du har lämnat, ii) vidta åtgärder för att skydda och stödja de personer som skyddas av lagstiftningen om visselblåsare, iii) följa upp rapporten och, om möjligt, vidta åtgärder för att svara på resultaten av en rapport, iv) vidta eventuella disciplinära åtgärder mot visselblåsaren som har rapporterat brottet med avsikt eller grov vårdslöshet eller mot berörda personer som är ansvariga för den rapporterade överträdelsen, v) använda resultaten av rapporter som bevis i rättsliga förfaranden.

Rättslig grund för behandlingen för ändamålen enligt i), ii) och iii) (i relation till syftena med att genomföra svarsåtgärder på resultatet av en rapport, strikt nödvändig för att undanröja konsekvenserna av den rapporterade överträdelsen) är behovet av att uppfylla de skyldigheter som den personuppgiftsansvarige föreskriver i lag, genom förordning eller annan lagstiftning.
I förhållande till syftena med att implementera svarsåtgärder på resultatet av en rapport, eventuellt annorlunda än de som är strikt nödvändiga för att undanröja konsekvenserna av den rapporterade överträdelsen, är den rättsliga grunden den personuppgiftsansvariges legitima intresse att förbättra organisationsstrukturen.
I förhållande till de disciplinära syftena är den rättsliga grunden den personuppgiftsansvariges legitima intresse att åtala eventuella brister i efterlevnaden av den personuppgiftsansvariges whistleblowing-procedur och/eller, mer generellt, av lagstiftningen som rör whistleblowing.
I förhållande till syftena med att använda data som bevis i rättsliga förfaranden är den rättsliga grunden den personuppgiftsansvariges legitima intresse att utöva försvaret av sina rättigheter.

Hållbarhet

Personuppgifter som mottagits av den personuppgiftsansvarige men som inte är absolut nödvändiga för utvärderingen av rapporten kommer att raderas omedelbart.
Rapporteringsuppgifterna och tillhörande dokumentation kommer att sparas så länge som det är nödvändigt för behandlingen av rapporten och under alla omständigheter inte senare än 5 (fem) år (i Italien), eller senast 2 (två) år (i Sverige), från den dag då det slutliga resultatet av rapporteringsförfarandet meddelades, med förbehåll för skyldigheterna att hålla informationen konfidentiell samt begränsningen av lagring, i enlighet med tillämpliga bestämmelser, och utöver denna period så länge det är nödvändigt för att slutföra ett redan påbörjat administrativt eller rättsligt förfarande eller för utredningsförfaranden enligt straffprocesslagen.

Rättigheter

Den rapporterande personen kan när som helst kontakta den personuppgiftsansvarige, utan formaliteter, för att utöva följande rättigheter: a) få tillgång till uppgifterna, b) rätta uppgifterna om de är felaktiga, c) uppdatera uppgifterna om de är föråldrade, d) begära radering av uppgifterna, e) begära begränsning av behandlingen av uppgifterna, f) när som helst invända mot behandlingen av uppgifterna av skäl som har samband med hans/hennes särskilda situation, g) få meddelande om ett dataintrång i det fall det innebär en hög risk för de berörda parternas grundläggande rättigheter eller friheter, h) (om Whistleblower har avslöjat sin identitet, eller, i fallet med en anonym anmälan, är detta möjligt även utan att avslöja sin identitet) kontrollera, korrigera och godkänna texten i en rapport som har transkriberats av den personuppgiftsansvarige efter tas emot i en form som inte kräver användning av en skriftlig form (t.ex. genom personligt möte, telefonsamtal eller annan oinspelad muntlig form, vanlig post). Återkallandet av samtycke påverkar inte lagligheten av den behandling och kommunikation som utförs på frivillig basis fram till återkallelsen.

Efter att ha begärt bevis på din identitet (om du inte har beslutat att vara anonym) kommer vi att bekräfta din begäran om att utöva dina rättigheter inom 30 dagar efter mottagandet av rapporten, om inte en särskild utredning är nödvändig, i vilket fall vi kommer att skicka ett meddelande till dig.

Så länge och i den utsträckning det är nödvändigt för att skydda identiteten för en whistleblower, för en annan skyddad subjekt enligt gällande lagstiftning, eller för personer som är intresserade av en uppföljningsåtgärd (t.), och att uppnå syftena att förhindra och bestraffa intrång, särskilt för att förhindra försök att förhindra, försämra eller fördröja informationen eller efterföljande åtgärder baserade på informationen, särskilt under varaktigheten av ett administrativt eller rättsligt förfarande eller ett preliminärt förfarande enligt brottsprocessbalken gäller inte följande rättigheter för en berörd fysisk person:

- Rätt till information, Rätt till rättelse, Rätt till radering, Rätt till begränsning av behandling, Rätt att invända, Rätt till anmälan om ett personuppgiftsintrång.

När ovanstående villkor uppstår kommer den personuppgiftsansvarige därför att avstå från att tillhandahålla information till en person som berörs av en Rapport.

Om rapportören anser att ovannämnda rättigheter har kränkts, kan denne alltid lämna in ett klagomål till den behöriga tillsynsmyndigheten.

I Italien är tillsynsmyndigheten Garante per la protezione dei dati personali med kontor Piazza Piazza Venezia, 11 - 00187 Roma (Italia), PEC: protocollo@pec.gpdp.it.

I Sverige är tillsynsmyndigheten Integritetsskyddsmyndigheten (YMY) - FE 7744 - 831 90 Östersund - Sverige
Telefonnummer: +46 (0)8 657 61 00; E-post: imy@imy.se; Postadress: Integritetsskyddsmyndigheten, Box 8114, 104 20 Stockholm, Sverige.