

PRIVACY INFORMATION (articles 13-14 GDPR)

This document contains the information required by articles 13 and 14 of EU Regulation 679/2016 (GDPR), in relation to the processing of personal data of data subjects who are involved, for various reasons, in reporting significant violations pursuant to the Whistleblowing Procedure of the Mastrotto Group.

Data Controller

The data controller is the company:

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

(in particular, each company is the Data Controller of data relating to reports of violations concerning its organization).

The DPO - Data Protection Officer designated by RINO MASTROTTO GROUP (Avv. Gianluigi Muscas) is domiciled and can be contacted at RINO MASTROTTO GROUP SPA. Co-ownership

Joint Data Controllers

The reports received will be managed through a centralized service in saas mode provided by RINO MASTROTTO SPA, also on behalf of the other subsidiaries of the Mastrotto Group. This service involves the processing of data shared between the subsidiaries and RINO MASTROTTO GROUP SPA, with the application of a joint controllership regime between them pursuant to art. 26 of the GDPR. For more details on the terms and conditions of the joint ownership agreement, consult the Group Whistleblowing Procedure on the website www.rinomastrottogroup.com, Whistleblowing section.

Personal data and optional provision

In principle, the whistleblowing system can be used without providing your own or third-party personal data. However, as part of the reporting process, you may voluntarily disclose personal data, in particular information about your identity, first and last name, country of residence, telephone number or email address.

Furthermore, as a rule, we do not request or process any particular category of personal data, for example about racial and/or ethnic origin, religious and/or philosophical beliefs, trade union membership or sex life or orientation. However, due to free text fields in the registration form, such special categories of personal data may be voluntarily disclosed by you, if you deem it necessary.

The report may also contain personal data of third parties.

The persons to whom the processed personal data refer are i) persons aware of the facts reported, or who are in any case requested to provide information following a report ii) "subjects involved" (i.e. blamed for the violation object of the report), iii) "protected persons" (i.e. who enjoy the mandatory protections provided for by the whistleblowing legislation in relation to a report), iv) Case Manager natural persons, v) other people who for various reasons can be made aware of the existence and follow-up of the report.

The data processed may include data and omissions punishable by a court or administrative authority, in particular also on suspicion of commission of crimes, and on criminal convictions or preventive

measures pursuant to art. 10 of the GDPR. Such data pursuant to art. 10 of the GDPR must be processed only in case of absolute necessity, are documented in writing and kept only to the extent strictly necessary after the decision on the offense has become final in a proceeding in which they were processed; storage takes place, if possible, without reprocessing.

The provision of your personal data is optional and therefore any failure to provide data will not affect your right to receive feedback after sending your report, and, if you have revealed your identity, to enjoy the protections provided by law.

Reporters who process personal data of their knowledge beyond what is necessary to follow up on the report, assume the role of Data Controllers pursuant to art. 4 n 7 of the GDPR.

Communication of personal data

In compliance with the protection of the confidentiality of the identity of the whistleblower, the Data Controller may share the data, in accordance with the principle of strict necessity, proportionality and minimization, with:

the. Other internal functions of the Data Controller, which the Case Managers of the same deem appropriate to involve in the investigation of a report.

ii. Case Manager, i.e. to the bodies, internal or external, designated by the receiving company to admit and/or examine the merits of the report and/or to adopt the consequent actions, including the response due to you.

iii. Third parties expressly designated as External Data Processors for hosting, maintenance or technical management purposes of the data center and of the online platform used by you to make the report and of the related database.

iv. Competent external authorities on a case-by-case basis based on the applicable regulations (e.g. judicial authorities, police bodies, financial police, ANAC - National Anti-Corruption Authority, etc.).

v. Law firms and/or consultants, corporate compliance consultants and/or other subjects involved in the process of evaluating the report (e.g. party experts, technical consultants, other companies of our group in which the investigation and decision-making activities of the reports, and/or who are in any capacity involved in a reported violation).

Technical implementation and security of your data

The online reporting channel includes an option for anonymous communication over an encrypted connection. When using the offense reporting system, the IP address and geolocation of the device you are using (PC, tablet, smartphone) are not stored at any time. We recommend that, if possible, you do not connect to the reporting system from a company device. When sending the report, you will need to create the password to access a Secure Inbox, in order to then be able to communicate with us in a secure way. It is your duty to adequately protect the confidentiality of both the identification code of the report you made (which will be communicated to you by our system), and the password to access the Secure Inbox. We maintain appropriate technical and organizational measures to ensure data protection and confidentiality. The internet communication channel used is encrypted using advanced protocols. The data will be stored in an encrypted format in an ISO 27001 certified data center located in Germany or Switzerland.

Personal data not necessary for the management of a Report will not be collected or will be immediately deleted if collected unintentionally.

The processing of personal data is lawful to the extent that it complies with a public interest for the purpose of preventing or punishing violations of the law, and in this context, to provide information and verify its validity.

For the purposes described above, the whistleblowers can carry out the processing of personal data, as regards the data required for their reporting.

Non-EEA data transfer

Any data transfers to countries outside the EEA area will be limited to the use of individual productivity cloud service based on data centers located in the U.S.A. (e.g. Microsoft Office 365) and in this case they will enjoy the guarantees established i) by the stipulation, between our company and the third party supplier, of standard contractual clauses compliant with the model approved by the EU Commission and/or ii) by the provisions of the bilateral agreement stipulated between the EU and the USA referred to as the "Trans-Atlantica Data Protection Framework" and/or by an adequacy decision of the EU Commission regarding the US privacy legislation (starting from its entry into force). In the case of data transfer to Switzerland, the guarantee of the transfer is the adequacy decision of the EU Commission regarding the Swiss privacy law.

The data may be transferred to the subsidiary companies that are the Data Controllers (or to other subjects authorized by them), based in the U.S.A., in Brazil and in Mexico, by the company RINO MASTROTTO GROUP SPA, as Data processor on behalf of the Data Controllers themselves on the basis of a contract for the assignment of centralized management services of the life cycle of reports of violations relating to these Data Controllers, by making access to the same data available through the saas Integrity Line service.

In this case the transfer is limited, from time to time, to the data concerning the reports relating to the single subsidiary and is assisted by the guarantee constituted by the stipulation, between the parties, of standard contractual clauses compliant with the model approved by the EU Commission.

The data will not be disclosed, except in the cases specifically provided for by national or European Union law.

Purpose and legal basis

The data will be processed to i) evaluate the admissibility and validity of the report of offenses communicated by you, ii) apply the protection and support measures of the subjects protected by the legislation on whistleblowing, iii) follow up on the report and, if possible, response measures to the results of a report, iv) apply any disciplinary measures against those who report with willful misconduct or gross negligence, or against any subjects involved who are responsible for the reported violation, v) use the results of reports as evidence in legal proceedings.

The Legal basis of the processing for the purposes under i), ii) and iii) (in relation to the purposes of implementing response measures to the results of a report, strictly necessary to remove the consequences of the reported Violation) is the need to fulfill the obligations provided for by the Data Controller by law, by a regulation or by other legislation.

In relation to the purposes of implementing response measures to the results of a report, possibly different from those strictly necessary to remove the consequences of the reported Violation, the legal basis is the legitimate interest of the Data Controller to improve the organization structure.

In relation to the disciplinary purposes, the legal basis is the legitimate interest of the Data Controller to prosecute any non-compliance with the Data Controller's Whistleblowing Procedure and/or, more generally, with the legislation relating to whistleblowing.

In relation to the purposes of using data as evidence in legal proceedings, the legal basis is the legitimate interest of the Data Controller to exercise the defense of their rights.

Duration of storage

Personal data received by the Data Controller but not strictly necessary for the evaluation of the report will be immediately cancelled.

The reporting data and related documentation will be kept for the time necessary to process the report and in any case no later than 5 (five) years (in Italy), or 2 (two) years (in Sweden), from the date of communication of the final outcome of the reporting procedure, in compliance with the confidentiality obligations of the information as well as limitation of conservation, provided for by the applicable regulations on the subject and beyond this period for as long as necessary for the completion of an

administrative or judicial proceeding already started or for investigative proceedings pursuant to the Criminal Procedure Code.

Rights

The whistleblower can contact the Data Controller at any time, without formalities, to exercise the following rights: a) access the data, b) rectify the data if inaccurate, c) update the data if obsolete, d) request the deletion of the data, and e) request the limitation of data processing, f) oppose the processing of data at any time for reasons deriving from one's particular situation, g) receive notification of a data breach in the event that the same involves a high risk for the fundamental rights or freedoms of the interested parties, h) (if the Whistleblower has revealed his identity, or, in the case of an anonymous Report, this is possible even without revealing his identity) check, correct and approve the text of a report that has been transcribed by the Data Controller after being received in a form that does not require the use of a written form (e.g. by personal meeting, telephone call or other unrecorded oral form, ordinary mail). The withdrawal of consent, if any, does not affect the lawfulness of the processing and communication carried out on a voluntary basis until such withdrawal.

Upon request for proof of your identity (unless you have decided to remain anonymous) we will respond to the request to exercise the rights within 30 days of receiving the report, unless particular in-depth analysis is necessary which, in this case, we will send a notice.

As long as and to the extent that it is necessary to protect the identity of a whistleblower, of another protected subject as defined by current legislation, or of persons interested in a follow-up action (e.g. case managers, persons informed of the reported facts), and to achieve the purposes of preventing and punishing Infringements, in particular to prevent attempts to prevent, impair or delay the Information or subsequent actions based on the Information, in particular for the duration of an administrative or judicial proceeding or a proceeding preliminary under the Criminal Procedure Code, the following rights of a natural person concerned do not apply:

- Right to information, Right to rectification, Right to erasure, Right to restriction of processing, Right to object, Right to notification of a personal data breach.

Therefore, upon occurrence of the above conditions, THE Data Controller will refrain from providing information to a person affected by a Report.

If the whistleblower believes that the aforementioned rights have been violated, he can always lodge a complaint with the competent Supervisory Authority.

In Italy, the competent Supervisory Authority is the Guarantor for the protection of personal data with offices in Piazza Venezia, 11 - 00187 Rome, PEC: protocol@pec.gpdp.it.

In Sweden, the competent Supervisory Authority is Integritetsskyddsmyndigheten (YMY) - FE 7744 - 831 90 Östersund - Sweden. Telephone: +46 (0)8 657 61 00; Email: imy@imy.se; Postal address: Integritetsskyddsmyndigheten, Box 8114, 104 20 Stockholm, Sweden.