RINO MASTROTTO

INFORMATION SECURITY POLICY

INFORMATION SECURITY POLICY

RINO MASTROTTO, recognized global leader in the provisioning of excellent materials to produce luxury goods, stands out for its offer of high-quality leathers for the leather goods, automotive, furniture and footwear sectors, as well as top quality fabrics and high value-added services.

Conscious of the strategic importance of the protection of personal data, RINO MASTROTTO (hereinafter also the Group) is committed to guaranteeing the highest level of security, in accordance with current regulations and internationally recognized standards.

This Policy applies to all Group companies, both in Italy and abroad, and is addressed to all stakeholders involved in the management of information of RINO MASTROTTO and/or its customers.
These include:

- employees, including fixed-term, part-time and similar workers
- collaborators working in the Group's plants
- all subjects who collaborate with RINO MASTROTTO directly or indirectly, continuously or occasionally (e.g., consultants, suppliers, agents, representatives and intermediaries)
- anyone who has commercial relations with the companies of the Group.

With this Policy, RINO MASTROTTO confirms its commitment to protecting the privacy and security of personal data, promoting responsible and transparent management of information in every operational area, as already expressly indicated in our Code of Ethics and Conduct, in force since 2012 and its subsequent updates, from which this Policy takes inspiration and expands the concepts.

With the adoption of this Policy, we have been inspired by the Principles of the Italian Data Protection Authority (both in Italy and in other jurisdictions, where national data protection authorities provide specific guidance) as well as by the main international guidelines and standards in the field of personal data protection that reflect best practices and offer a regulatory framework to ensure data security and responsible management.

With respect to the international regulatory framework:

- GDPR (General Data Protection Regulation), the European Union regulation that regulates the protection of the personal data of European citizens. It includes principles such as consent, purpose limitation, data minimization, and the right to be erasure.
- LGPD (Lei Geral de Proteção de Dados), Brazil's data protection law, inspired by the GDPR.

With respect to standards and best practices:

- ISO 27001:2022, an international standard for information security management, which provides a systematic approach to data protection and information security.
- TISAX (Trusted Information Security Assessment Exchange) - an international standard specific to information security management, developed to meet the needs of the automotive industry. Created on the basis of the ISO 27001 standard and adapted to the peculiarities of the automotive supply chain, as required by the VDA (Verband der Automobilindustrie), the German association of the automotive industry.
- NIST Privacy Framework, developed by the National Institute of Standards and Technology (NIST), which guides organizations in managing privacy-related risks.
- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - OECD Guidelines to facilitate the protection of privacy in cross-border data flows.

The Information Security Management System (hereinafter also ISMS) is the tool with which RINO MASTROTTO intends to protect the confidentiality, integrity and availability of its information assets, including the sensitive information of its customers and suppliers. The achievement of adequate levels of security allows our group to mitigate and contrast losses and damages that may have an impact on people, on the image and reputation of the company, on economic

and financial aspects, as well as ensure the compliance with the contractual and legislative context in force on the protection of information and personal data.

RINO MASTROTTO applies the following principles:

DATA MINIMISATION

Minimisation of the amount of personal data collected and used in our operations, limiting to what is strictly necessary to provide our services and to comply with our contractual and legal obligations. We only keep data for as long as necessary and safely erase it when it is no longer needed.

DATA PROTECTION

Implementation of technical, organizational, and procedural security measures to protect personal data from unauthorized access, loss, manipulation, or improper disclosure. We use advanced technologies such as encryption, firewalls, monitoring, and authentication to ensure the security and integrity of data to safeguard company, customer, and supplier information, preserving confidentiality, integrity, and availability at every stage of their lifecycle.

CONTROLLED ACCESS

We limit access to personal data to only authorized persons who need it to perform their activities and based on operational needs. We implement access and authorization controls based on the principle of least privilege to ensure that only authorized persons can access personal data, preventing unauthorized access both internal and external.

ADEQUATE SECURITY MEASURES

We want to establish, implement, and maintain specific security measures to prevent breaches, abuse, fraud, and other threats that may compromise information.

ROLES AND RESPONSIBILITIES

Assign clear and defined roles and responsibilities for the management and protection of data, involving both internal staff and external collaborators.

TRAINING AND AWARENESS

We provide continuous and specific training to raise awareness among our employees and collaborators on best practices in data protection, including privacy regulations and the management of risks related to information security. We promote a corporate culture of security and privacy, encouraging our employees to be aware of the risks and responsibilities associated with the management of personal data.

BUSINESS CONTINUITY AND INCIDENT MANAGEMENT

RINO MASTROTTO guarantees information security even in emergency situations or adverse scenarios, through business continuity and emergency management plans.

We are ready to deal with any data security breaches with a well-defined incident management procedure. We respond promptly to security breaches, investigating the causes, mitigating the damage and notifying the relevant authorities and affected parties if necessary.

COMPLIANCE WITH STANDARDS

Ensure compliance with relevant regulations and standards, in particular ISO 27001 and TISAX, and adopt industry best practices for data protection.

COMPLIANCE WITH LAWS AND REGULATIONS

RINO MASTROTTO acts in compliance with the laws, regulations and contractual provisions in force, with particular attention to the protection of personal data and the processing of information, ensuring the appropriate custody of personal and third-party information according to the principles of lawfulness, proportionality and relevance.

We are committed to complying with all applicable data protection regulations, including the European Union's General Data Protection Regulation (GDPR) and other privacy laws at global level. We maintain a continuous update on the new regulations and adapt our policies and procedures accordingly.

ASSESSMENT AND CONTINUOUS IMPROVEMENT

Promoting a process of continuous improvement of the ISMS, through the monitoring, review and periodic updating of the security measures implemented is one of the priorities we have set. We constantly monitor our data protection policies, procedures, and practices to assess their effectiveness and identify areas for improvement. We regularly conduct internal audits and performance reviews to ensure the respect of our standards and that our security measures are adequate.

RINO MASTROTTO intends to achieve the information security objectives described by means of a structured risk management approach, integrated into business processes and aimed at ensuring protection, business continuity and regulatory compliance. This approach is based on:

- identification and assessment of risks with analysis of systems, infrastructures and data flows to identify threats and vulnerabilities, ranking risks by priority;
- mitigation measures such as the planning of technological (firewall, encryption, backup), organizational (access policies, standard procedures) and physical (access controls, environmental protections) interventions;
- monitoring and updating through periodic checks on the effectiveness of the measures adopted and continuous adaptation to new threats or regulatory requirements;
- safety culture through the direct involvement of all company levels by means of training and awareness-raising.

ADOPTION, IMPLEMENTATION AND DISSEMINATION

This policy is communicated to all staff and made available to interested parties, if necessary. The recipients are required to know the contents of the Social Policy, are obliged to observe the principles contained in it, and are called to actively promote its observance.

RINO MASTROTTO **will not tolerate any kind of violation of this policy**.

With this aim, RINO MASTROTTO is committed to ensure the maximum dissemination of this Policy, through the use of adequate and training tools and promoting the awareness of its contents, by means of training sessions provided for personnel, the posting of the same on the appropriate company bulletin boards rather than through publication on the company's website (www.rinomastrotto.com).

RINO MASTROTTO is committed to maintaining constant and transparent communication with its stakeholders, listening to the needs of all internal and external stakeholders, to ensure the correct implementation of the Policy and facilitate their commitment.

The Management of RINO MASTROTTO:

- is directly responsible for the implementation of this policy and its compliance by all interested parties;
- shares the principles and objectives of the ISMS, supporting its implementation through the allocation of adequate resources;
- supports continuous improvement, ensuring that the ISMS remains effective, appropriate and aligned with business and regulatory needs.

It is attributed to appropriate management figures, such as managers and function or area managers, the role of applying the principles included in the Policy, as they are involved in the daily supervision of personnel, suppliers and customers.

With this policy, RINO MASTROTTO reaffirms its commitment to responsible and secure information management, which is essential to sustain the trust of customers, suppliers and partners in a context of continuous change and increasing digitalisation. This policy is submitted to periodic review with the possibility to modify any procedures if deemed appropriate, including, but not limited to, changes required by local legal or regulatory requirements.

This Policy approved by the Board of Directors on 26th of August 2024, will be regularly updated whenever deemed necessary to reflect ongoing developments in ESG and best practice developments.