



RINO MASTROTTO

POLITICA PER LA SICUREZZA  
DELLE INFORMAZIONI

# POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

**RINO MASTROTTO**, leader globale riconosciuto nella fornitura di materiali di eccellenza destinati alla produzione di beni di lusso, si distingue per l'offerta di pelli di alta qualità per i settori della pelletteria, dell'automotive, dell'arredamento e della calzatura, nonché di tessuti di pregio e servizi ad alto valore aggiunto.

Conscia della rilevanza strategica della protezione dei dati personali, RINO MASTROTTO (di seguito anche il Gruppo) si impegna a garantire il massimo livello di sicurezza, in conformità con le normative vigenti e gli standard internazionalmente riconosciuti.

La presente Politica si applica a tutte le società del Gruppo, sia in Italia che all'estero, ed è rivolta a tutti gli stakeholder coinvolti nella gestione di informazioni di RINO MASTROTTO e/o dei suoi clienti.

Tra questi figurano:

- il personale dipendente, compresi lavoratori a tempo determinato, part-time e assimilati
- i collaboratori operanti presso le sedi del Gruppo
- tutti i soggetti che collaborano con RINO MASTROTTO in modo diretto o indiretto, continuativo o occasionale (ad esempio, consulenti, fornitori, agenti, rappresentanti e intermediari)
- chiunque intrattenga rapporti commerciali con le società del Gruppo.

Attraverso questa Politica, RINO MASTROTTO ribadisce il proprio impegno a tutelare la privacy e la sicurezza dei dati personali, promuovendo una gestione responsabile e trasparente delle informazioni in ogni ambito operativo, come già espressamente indicato nel nostro Codice Etico e di Condotta, in uso fin dal 2012 e suoi successivi aggiornamenti, dal quale la presente politica prende spunto e ne amplia i concetti.

Nell'adottare questa politica, ci siamo ispirati ai Principi del Garante per la Protezione dei Dati Personali (sia in Italia e in altre giurisdizioni, dove i garanti nazionali forniscono orientamenti specifici) nonché alle principali linee guida e standard internazionali nel campo della protezione dei dati personali che riflettono le migliori pratiche e offrono un quadro normativo per garantire la sicurezza e la gestione responsabile dei dati.

Rispetto al quadro normativo internazionale:

- GDPR (General Data Protection Regulation), il regolamento dell'Unione Europea che disciplina la protezione dei dati personali dei cittadini europei. Include principi come il consenso, la limitazione delle finalità, la minimizzazione dei dati e il diritto all'oblio.
- LGPD (Lei Geral de Proteção de Dados), la legge brasiliana sulla protezione dei dati, ispirata al GDPR.

Rispetto a standard e best practices:

- ISO 27001:2022, standard internazionale per la gestione della sicurezza delle informazioni, che fornisce un approccio sistematico alla protezione dei dati e alla sicurezza delle informazioni.
- TISAX (Trusted Information Security Assessment Exchange) - standard internazionale specifico per la gestione della sicurezza delle informazioni, sviluppato per soddisfare le esigenze del settore automobilistico. Creato sulla base della norma ISO 27001 e adattato alle peculiarità della filiera automotive, come richiesto dalla VDA (Verband der Automobilindustrie), l'associazione tedesca dell'industria automobilistica.
- NIST Privacy Framework, sviluppato dal National Institute of Standards and Technology (NIST), che guida le organizzazioni nella gestione dei rischi legati alla privacy.
- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - Linee guida dell'OCSE per facilitare la protezione della privacy nei flussi transfrontalieri di dati.

Il Sistema di Gestione della Sicurezza delle Informazioni (di seguito anche SGSI) è lo strumento con il quale RINO MASTROTTO intende proteggere la riservatezza, l'integrità e la disponibilità del proprio patrimonio informativo, ivi incluse le informazioni sensibili dei suoi clienti e fornitori. Il raggiungimento di adeguati livelli di sicurezza, consente al nostro gruppo di mitigare e contrastare perdite e danneggiamenti che possano avere impatto sulle persone,

sull'immagine e la reputazione aziendale, sugli aspetti di natura economica e finanziaria, oltre a consentire la conformità al contesto contrattuale e legislativo vigente in materia di protezione delle informazioni e dei dati personali.

RINO MASTROTTO mette in pratica i seguenti principi:

#### **MINIMIZZAZIONE DEI DATI**

Riduciamo al minimo la quantità di dati personali raccolti e utilizzati nelle nostre operazioni, limitandoci a ciò che è strettamente necessario per fornire i nostri servizi e per adempiere ai nostri obblighi contrattuali e legali. Manteniamo i dati solo per il periodo di tempo necessario e li eliminiamo in modo sicuro quando non sono più necessari.

#### **PROTEZIONE DELLE INFORMAZIONI**

Implementiamo misure di sicurezza tecniche, organizzative e procedurali per proteggere i dati personali da accessi non autorizzati, perdite, manipolazioni o divulgazioni indebite. Utilizziamo tecnologie avanzate di crittografia, firewall, monitoraggio e autenticazione per garantire la sicurezza e l'integrità dei dati con il fine di salvaguardare le informazioni aziendali, dei clienti e dei fornitori, preservandone riservatezza, integrità e disponibilità in ogni fase del loro ciclo di vita.

#### **ACCESSO CONTROLLATO**

Limitiamo l'accesso ai dati personali solo alle persone autorizzate che ne hanno bisogno per svolgere le proprie mansioni e in base a necessità operative. Implementiamo controlli di accesso e autorizzazioni basati sul principio del minimo privilegio per garantire che solo le persone autorizzate possano accedere ai dati personali, prevenendo accessi non autorizzati sia interni che esterni.

#### **MISURE DI SICUREZZA ADEGUATE**

Vogliamo definire, attuare e mantenere misure di sicurezza specifiche per prevenire infrazioni, abusi, frodi e altre minacce che possano compromettere le informazioni.

#### **RUOLI E RESPONSABILITÀ**

Assegnare ruoli e responsabilità chiari e definiti per la gestione e la protezione delle informazioni, coinvolgendo sia il personale interno che i collaboratori esterni.

#### **FORMAZIONE, SENSIBILIZZAZIONE E CONSAPEVOLEZZA**

Forniamo formazione continua e specifica per sensibilizzare i nostri dipendenti e i nostri collaboratori sulle migliori pratiche di protezione dei dati, comprese le normative sulla privacy e la gestione dei rischi relativi alla sicurezza delle informazioni. Promuoviamo una cultura aziendale orientata alla sicurezza e alla privacy, incoraggiando i nostri dipendenti a essere consapevoli dei rischi e delle responsabilità associate alla gestione dei dati personali.

#### **GESTIONE DELLA CONTINUITÀ E DEGLI INCIDENTI**

RINO MASTROTTO garantisce la sicurezza delle informazioni anche in situazioni di emergenza o scenari avversi, attraverso piani di continuità operativa e gestione delle crisi.

Siamo pronti ad affrontare eventuali violazioni della sicurezza dei dati con una procedura di gestione degli incidenti ben definita. Rispondiamo tempestivamente alle violazioni della sicurezza, investigando sulle cause, mitigando i danni e notificando le autorità competenti e gli interessati, se necessario.

#### **CONFORMITÀ AGLI STANDARD**

Assicurare il rispetto delle normative e degli standard di riferimento, in particolare ISO 27001 e TISAX, e adottare le migliori pratiche del settore per la protezione dei dati.

#### **CONFORMITÀ NORMATIVA**

RINO MASTROTTO opera in conformità alle disposizioni legislative, regolamentari e contrattuali vigenti, con particolare attenzione alla protezione dei dati personali e al trattamento delle informazioni garantendo la idonea custodia delle informazioni personali e di terzi secondo i principi di liceità, proporzionalità e pertinenza.

Ci impegniamo a rispettare tutte le normative applicabili in materia di protezione dei dati, inclusi il Regolamento Generale sulla Protezione dei Dati (GDPR) dell'Unione Europea e altre leggi sulla privacy a livello globale. Manteniamo un costante aggiornamento sulle nuove normative e adattiamo le nostre politiche e procedure di conseguenza.

## VALUTAZIONE E MIGLIORAMENTO CONTINUO

Promuovere un processo di miglioramento continuo del SGSI, attraverso il monitoraggio, la revisione e l'aggiornamento periodico delle misure di sicurezza implementate è una delle priorità che ci siamo posti. Monitoriamo costantemente le nostre politiche, procedure e pratiche di protezione dei dati per valutare la loro efficacia e identificare le aree di miglioramento. Effettuiamo regolarmente audit interni e revisioni delle prestazioni per garantire il rispetto dei nostri standard e l'adeguatezza delle nostre misure di sicurezza.

RINO MASTROTTO intende raggiungere gli obiettivi di sicurezza delle informazioni fin qui descritti attraverso un approccio strutturato di gestione del rischio, integrato nei processi aziendali e mirato a garantire protezione, continuità operativa e conformità normativa. Questo approccio si basa su:

- identificazione e valutazione dei rischi con analisi dei sistemi, infrastrutture e flussi di dati per individuare minacce e vulnerabilità, classificando i rischi per priorità;
- misure di mitigazione come la pianificazione di interventi tecnologici (firewall, crittografia, backup), organizzativi (policy di accesso, procedure standard) e fisici (controlli di accesso, protezioni ambientali);
- monitoraggio e aggiornamento attraverso verifiche periodiche dell'efficacia delle misure adottate e adattamento continuo a nuove minacce o requisiti normativi;
- cultura della sicurezza tramite il coinvolgimento attivo di tutti i livelli aziendali attraverso formazione e sensibilizzazione.

## ADOZIONE, IMPLEMENTAZIONE E DIVULGAZIONE

La presente politica è comunicata a tutto il personale e resa disponibile alle parti interessate, qualora necessario. I destinatari sono tenuti a conoscere i contenuti della presente Politica, obbligati a osservare i principi in essa contenuti, nonché chiamati a promuoverne attivamente la sua osservanza.

**RINO MASTROTTO non tollererà alcun tipo di violazione della presente politica.**

A tal fine RINO MASTROTTO si impegna ad assicurare la massima diffusione della presente Politica, attraverso l'utilizzo di adeguati strumenti conoscitivi e formativi e la sensibilizzazione in merito ai suoi contenuti, tramite le sessioni di formazione previste per il personale, l'affissione della stessa nelle apposite bacheche aziendali piuttosto che tramite la pubblicazione nel sito internet della società ([www.rinomastrotto.com](http://www.rinomastrotto.com)).

RINO MASTROTTO si impegna a mantenere una comunicazione costante e trasparente con i suoi stakeholder, ascoltando le esigenze di tutte le parti interessate interne ed esterne, al fine di assicurare una corretta implementazione della Politica e facilitare l'impegno da parte degli stessi.

La Direzione di RINO MASTROTTO:

- è direttamente responsabile dell'attuazione della presente politica e della sua osservanza da parte di tutte le parti interessate;
- condivide i principi e gli obiettivi del SGSI, supportandone la realizzazione attraverso l'allocatione di risorse adeguate;
- sostiene il miglioramento continuo, garantendo che il SGSI resti efficace, idoneo e allineato con le esigenze aziendali e normative.

Viene attribuito a proprie figure dirigenziali, quali manager e responsabili di funzione o di area, il ruolo di applicare i principi previsti dalla Politica, in quanto coinvolti nella supervisione quotidiana del personale dei fornitori, dei clienti.

Con questa politica, il RINO MASTROTTO riafferma il proprio impegno verso una gestione responsabile e sicura delle informazioni, fondamentale per sostenere la fiducia di clienti, fornitori e partner in un contesto di continuo cambiamento e crescente digitalizzazione. Si sottopone la presente politica a riesame periodico con la possibilità di modificare eventuali procedure qualora sia ritenuto appropriato, comprese, ma non limitatamente a modifiche richieste da requisiti legali o normativi locali.

La presente Politica approvata dalla Direzione in data 26 agosto 2024 verrà pertanto aggiornata periodicamente o straordinariamente in caso di cambiamenti significativi, al fine di assicurarne la continua adeguatezza ed efficacia.