

ITALIANO	ENGLISH
CODICE ETICO E DI CONDOTTA AZIENDALE INTEGRATO TMV MOLINARI S.R.L.	INTEGRATED CORPORATE CODE OF ETHICS AND CONDUCT OF TMV MOLINARI S.R.L. (THE ITALIAN VERSION IS THE RELEVANT ONE)
REVISIONE REQUISITI COMPLETI 2026	FULL REQUIREMENTS REVISION 2026
Approvato con Delibera del Consiglio di Amministrazione in data 15 Luglio 2026. Entrata in vigore immediata con efficacia vincolante globale per tutte le unità operative e le filiere di fornitura nazionali ed estere.	Approved by resolution of the Board of Directors on 15 July 2026. Effective immediately with globally binding effect for all operating units and national and foreign supply chains.
PREAMBOLO ISTITUZIONALE E PROFILO SOCIETARIO	INSTITUTIONAL PREAMBLE AND CORPORATE PROFILE
Fondata nel 1981, la TMV Molinari S.r.l. (di seguito denominata "Società" o "Azienda") si è affermata sul mercato globale come leader nella pianificazione, fabbricazione e fornitura di tiranteria e componentistica meccanica speciale destinata ad applicazioni industriali ad altissima responsabilità nei settori Oil & Gas, chimico, petrolchimico e navale. La sede legale e l'insediamento industriale della Società sono radicati in Località Colombarola, Via dell'Industria, 13-14 - 29010 Gragnano Trebbiense (PC) - ITALY.	Founded in 1981, TMV Molinari S.r.l. (hereinafter referred to as the "Company" or the "Business") has established itself in the global market as a leader in the planning, manufacture and supply of special bolting and mechanical components intended for very high-responsibility industrial applications in the Oil & Gas, chemical, petrochemical and naval sectors. The registered office and industrial site of the Company are located at Località Colombarola, Via dell'Industria, 13-14, 29010 Gragnano Trebbiense (PC), Italy.
La visione strategica di lungo periodo della Società unisce la tradizione manifatturiera e la qualità del Made in Italy con un costante investimento in alta tecnologia, digitalizzazione dei processi e valorizzazione delle risorse umane. TMV Molinari opera con il preciso obiettivo di offrire al mercato globale un prodotto caratterizzato da un elevato standard qualitativo a un prezzo concorrenziale, distinguendosi per l'estrema flessibilità operativa e per un'attiva, trasparente collaborazione tecnica con i propri clienti.	The Company's long-term strategic vision combines manufacturing tradition and the quality of Made in Italy with continuous investment in high technology, process digitalisation and the enhancement of human resources. TMV Molinari operates with the precise aim of offering the global market a product characterised by a high quality standard at a competitive price, distinguishing itself through extreme operational flexibility and active, transparent technical collaboration with its customers.
Il presente Codice Etico e di Condotta Aziendale Integrato non costituisce un mero manifesto di principi di facciata, bensì rappresenta il testo normativo dell'organizzazione. Esso unisce e integra in un unico corpo precettivo le politiche aziendali interne, le direttive ambientali, le norme di condotta ICT, i requisiti di compliance internazionale e le procedure di whistleblowing. L'osservanza del presente Codice è condizione imprescindibile per il mantenimento di qualsiasi rapporto lavorativo, professionale o commerciale con la Società.	This Integrated Corporate Code of Ethics and Conduct does not constitute a mere statement of superficial principles but represents the organization's normative text. It combines and integrates into a single prescriptive body the Company's internal policies, environmental directives, ICT rules of conduct, international compliance requirements and whistleblowing procedures. Compliance with this Code is an essential condition for maintaining any employment, professional or commercial relationship with the Company.
SEZIONE I: PRINCIPI GENERALI E MODELLO DI GOVERNANCE PREDITTIVA	SECTION I: GENERAL PRINCIPLES AND PREDICTIVE GOVERNANCE MODEL
Articolo 1 – Ambito di Applicazione, Destinatari e Vincolatività Contrattuale	Article 1 – Scope of Application, Addressees and Contractual Binding Effect
1.1 Le disposizioni e i precetti contenuti nel presente Codice Etico e di Condotta sono vincolanti, senza alcuna eccezione o deroga, per tutti i soggetti che operano in nome, per conto o nell'interesse della Società. Nello specifico, la qualifica di Destinatario si applica a:	1.1 The provisions and precepts contained in this Code of Ethics and Conduct are binding, without any exception or derogation, on all persons who operate in the name, on behalf of or in the interest of the Company. Specifically, the status of Addressee applies to:
Tutti i componenti del Consiglio di Amministrazione (CdA) e gli amministratori investiti di	All members of the Board of Directors (BoD) and directors vested with specific operational powers.

ITALIANO	ENGLISH
particolari deleghe operative.	
Tutti i membri del Collegio Sindacale e i soggetti incaricati della revisione legale dei conti.	All members of the Board of Statutory Auditors and the persons appointed to perform the statutory audit of the accounts.
I dirigenti, i quadri e l'intera platea dei dipendenti, sia a tempo determinato che indeterminato, operanti in Italia o all'estero e regolati dal CCNL Metalmeccanico.	Managers, middle managers and the entire body of employees, whether employed for a fixed term or indefinitely, operating in Italy or abroad and governed by the Metalworking National Collective Bargaining Agreement.
Tutti i collaboratori esterni, i consulenti, gli agenti, i procacciatori d'affari, i partner commerciali e i lavoratori in regime di somministrazione.	All external collaborators, consultants, agents, business introducers, commercial partners and agency workers.
Tutti i fornitori di materie prime, semilavorati e servizi che compongono la catena di approvvigionamento (Supply Chain), con menzione tassativa per le fonderie, le acciaierie e i laboratori partner esterni di prova e taratura.	All suppliers of raw materials, semi-finished products and services forming part of the supply chain, with mandatory express reference to foundries, steel mills and external partner laboratories for testing and calibration.
1.2 L'accettazione e il rispetto del presente Codice costituiscono parte integrante delle obbligazioni contrattuali dei dipendenti (ai sensi e per gli effetti degli articoli 2104 e 2105 del Codice Civile) e delle condizioni essenziali di validità dei contratti stipulati con terzi esterni. La mancata sottoscrizione o la violazione accertata dei suoi precetti legittima l'attivazione immediata delle tutele sanzionatorie e risolutive previste dalla legge e dal presente testo.	1.2 Acceptance of and compliance with this Code form an integral part of the contractual obligations of employees, pursuant to and for the purposes of Articles 2104 and 2105 of the Italian Civil Code, and of the essential conditions of validity of contracts entered into with external third parties. Failure to sign, or an ascertained breach of its precepts, entitles the Company to immediately activate the sanctions and termination remedies provided for by law and by this text.
Articolo 2 – La Governance Predittiva	Article 2 – Predictive Governance
2.1 la Società rifiuta categoricamente una conduzione aziendale orientata in modo esclusivo ai soli risultati economico-finanziari consuntivi (Backward-Looking), ritenuti insufficienti a garantire la continuità d'impresa in mercati ad alta volatilità. La pianificazione e il controllo di gestione si basano sul monitoraggio in tempo reale di indicatori prospettici (Forward-Looking) estrapolati dai dati del sistema ERP/MES/DMS e rapporti relazionali con i clienti.	2.1 The Company categorically rejects corporate management directed exclusively at ex post economic and financial results (backward-looking), which are considered insufficient to ensure business continuity in highly volatile markets. Planning and management control are based on real-time monitoring of perspective indicators (forward-looking) extrapolated from ERP/MES/DMS system data and from relationships with customers.
2.2 Il Consiglio di Amministrazione analizza e valuta con cadenza mensile i rischi strutturali, operativi, reputazionali e di mercato, unendo i dati contabili tradizionali con l'andamento e la proiezione dei seguenti Key Performance Indicators (KPI) operativi:	2.2 The Board of Directors analyses and assesses structural, operational, reputational and market risks monthly, combining traditional accounting data with the trend and projection of the following operational Key Performance Indicators (KPIs):
Efficienza dei processi e scarti industriali: misurazione analitica dei tassi di difettosità dei processi produttivi in piena conformità ai requisiti di miglioramento continuo dettati dalla certificazione di gestione della qualità.	Process efficiency and industrial scrap: analytical measurement of defect rates in production processes in full compliance with the continuous improvement requirements imposed by quality management certification.
Sicurezza informatica e resilienza cyber: monitoraggio dei tentativi di intrusione, integrità dei backup, aggiornamento dei sistemi di protezione e tracciabilità log, in conformità agli standard internazionali ISO/IEC 27001:2022.	Information security and cyber resilience: monitoring of intrusion attempts, backup integrity, updating of protection systems and log traceability, in accordance with international standard ISO/IEC 27001:2022.

ITALIANO	ENGLISH
Performance di sostenibilità e impronta ambientale & ESG: verifica costante del mantenimento dei target di decarbonizzazione stabiliti in linea con la direttiva europea CSRD / ESRS e certificati ai sensi della norma ISO 14067:2018 ed/o ESG (Environment Social Responsibilities, Governance) Synesgy certificate.	Sustainability performance and environmental & ESG footprint: constant verification that decarbonisation targets established in line with the European CSRD / ESRS Directive are maintained and certified pursuant to ISO 14067:2018 and/or ESG (Environmental, Social Responsibilities, Governance) Synesgy certificate.
Articolo 3 – Doppia Materialità ed Etica dell'Impatto (Direttiva CSRD / ESRS)	Article 3 – Double Materiality and Ethics of Impact (CSRD / ESRS Directive)
3.1 In stretta applicazione dei requisiti normativi comunitari introdotti dalla Corporate Sustainability Reporting Directive (CSRD), la Società mappa e definisce i propri obiettivi etici, sociali e di governance applicando rigorosamente il principio della Doppia Materialità: - Materialità d'Impatto (Inside-Out): Identificazione, valutazione e mitigazione sistematica degli impatti attuali o potenziali, positivi e negativi, generati dall'insediamento industriale e dalle lavorazioni metallurgiche di Gragnano Trebbiense (PC) sull'ambiente circostante, sulla biodiversità locale, sulle matrici ambientali (aria, acqua, suolo) e sulle persone (lavoratori, comunità locale, clienti). - Materialità Finanziaria (Outside-In): Analisi predittiva di come i fattori e i macro-trend ESG esterni possano influenzare la stabilità economica, l'accesso al credito, i costi assicurativi e la continuità finanziaria della Società nel lungo periodo. Tale analisi include specificamente l'impatto dell'introduzione di carbon tax o barriere doganali ecologiche sui mercati internazionali della tiranteria speciale, nonché il rischio geopolitico di carenza o interruzione nell'approvvigionamento di acciai speciali ad alta tecnologia per il comparto Oil & Gas.	3.1 In strict application of the EU regulatory requirements introduced by the Corporate Sustainability Reporting Directive (CSRD), the Company maps and defines its ethical, social and governance objectives by rigorously applying the principle of Double Materiality: - Impact Materiality (Inside-Out): systematic identification, assessment and mitigation of actual or potential, positive and negative impacts generated by the industrial site and metallurgical operations of Gragnano Trebbiense (PC) on the surrounding environment, local biodiversity, environmental matrices (air, water, soil) and people (workers, local community, customers). - Financial Materiality (Outside-In): predictive analysis of how external ESG factors and macro-trends may affect the Company's economic stability, access to credit, insurance costs and long-term financial continuity. This analysis specifically includes the impact of the introduction of carbon taxes or environmental customs barriers on the international markets for special bolting, as well as the geopolitical risk of shortage or disruption in the procurement of high-technology special steels for the Oil & Gas sector.
Articolo 4 – Certificazioni di Sistema e l'Impronta di Carbonio Fissa	Article 4 – Management System Certifications and Fixed Carbon Footprint
4.1 La Società considera le certificazioni internazionali rilasciate da enti terzi indipendenti ed accreditati come lo strumento fondamentale per comprovare sul mercato globale la serietà, la sostenibilità e l'eccellenza dei propri processi produttivi. I pilastri del sistema di gestione integrato sono costituiti da: - Certificazione ISO 9001: Garanzia assoluta del controllo dei processi di approvvigionamento, produzione e collaudo finale della tiranteria. - Certificazione PED (Pressure Equipment Directive): Requisito obbligatorio e vincolante per la fornitura di componenti destinati a recipienti in pressione, scambiatori di calore e sistemi di tubazioni industriali. - Certificazione ISO 14067:2018 (Greenhouse Gases - Carbon Footprint of Products): Strumento di quantificazione scientifica delle emissioni di gas a effetto serra associate all'intero ciclo di vita dei prodotti.	4.1 The Company regards international certifications issued by independent and accredited third-party bodies as the fundamental instrument for proving to the global market the seriousness, sustainability and excellence of its production processes. The pillars of the integrated management system consist of: - ISO 9001 certification: absolute guarantee of control over the procurement, production and final inspection processes for bolting. - PED certification (Pressure Equipment Directive): a mandatory and binding requirement for the supply of components intended for pressure vessels, heat exchangers and industrial piping systems. - ISO 14067:2018 certification (Greenhouse Gases — Carbon Footprint of Products): a scientific quantification instrument for greenhouse gas emissions associated with the entire life cycle of products.

ITALIANO	ENGLISH
Certificazione in accordo ai principi principi ESG (Synesgy) La sostenibilità ambientale, il benessere delle persone e l'etica di governance sono elementi fondanti del proprio produttivo nella fabbricazione di bulloneria e componenti speciali. In linea con i GRI e VSME. 4.2 In attuazione delle proprie politiche ambientali di massima trasparenza, la Società ha stabilito ed è tenuta a mantenere un'impronta di carbonio fissa certificata pari a 0,69 kg CO₂eq per sistema prodotto. Qualsiasi modifica dei processi di acquisto, logistica, produzione o imballaggio deve essere preventivamente vagliata dal CdA al fine di garantire il non superamento di tale soglia o l'adozione di immediate misure compensative basate su crediti di carbonio certificati o efficientamento energetico diretto.	Certification in accordance with ESG principles (Synesgy): environmental sustainability, people's well-being and governance ethics are foundational elements of the Company's production process in the manufacture of bolting and special components, in line with GRI and VSME. 4.2 In implementation of its environmental policies of maximum transparency, the Company has established and is required to maintain a certified fixed carbon footprint of 0.69 kg CO₂eq per product system. Any change to purchasing, logistics, production or packaging processes must be submitted in advance to the Board of Directors in order to ensure that this threshold is not exceeded or that immediate compensatory measures based on certified carbon credits or direct energy efficiency are adopted.
SEZIONE II: PROTEZIONE DEI DATI PERSONALI, SENSIBILI E PARTICOLARI (GDPR REGOLEMENTO UE 2016/679) Nel contesto dei moderni flussi informatici applicati alla progettazione su specifica del cliente, alla digitalizzazione dei laboratori e all'automazione dei reparti produttivi tramite sistemi interconnessi, la protezione dei dati personali è elevata a pilastro fondamentale di condotta morale e responsabilità giuridica della Società, in piena e rigorosa conformità al GDPR (Regolamento UE 2016/679).	SECTION II: PROTECTION OF PERSONAL, SENSITIVE AND SPECIAL CATEGORY DATA (GDPR, EU REGULATION 2016/679) In the context of modern information flows applied to customer-specific design, laboratory digitalisation and the automation of production departments through interconnected systems, the protection of personal data is elevated to a fundamental pillar of the Company's moral conduct and legal responsibility, in full and rigorous compliance with the GDPR (EU Regulation 2016/679).
Articolo 5 – Principi Generali di Trattamento, Liceità e Trasparenza 5.1 Liceità e Trasparenza: Ogni trattamento di dati personali riferito a dipendenti, collaboratori, candidati all'assunzione, clienti, rappresentanti di enti di collaudo e ispezione o fornitori deve basarsi su presupposti giuridici certi, espliciti e legittimi. È fatto obbligo di rilasciare preliminarmente al soggetto interessato un'apposita e dettagliata informativa scritta ai sensi dell'Articolo 13 del GDPR, specificando finalità, modalità, tempi di conservazione e diritti esercitabili. 5.2 Privacy by Design e by Default: L'architettura complessiva dei sistemi informatici aziendali – inclusi il sistema gestionale ERP, i database PDM (Product Data Management), le cartelle di rete condivise e i sistemi di posta elettronica – deve essere nativamente progettata e configurata in modo tale da minimizzare il trattamento dei dati personali, escludendo la raccolta di informazioni non strettamente necessarie. Di default, l'Azienda garantisce la cifratura forte dei database contenenti record personali, l'adozione di tecniche di pseudonimizzazione dei file sensibili e il rigido isolamento logico dei server per prevenire accessi non autorizzati, alterazioni o incidenti informatici (Data Breach).	Article 5 – General Principles of Processing, Lawfulness and Transparency 5.1 Lawfulness and Transparency: Any processing of personal data relating to employees, collaborators, job applicants, customers, representatives of testing and inspection bodies or suppliers must be based on certain, explicit and legitimate legal grounds. It is mandatory to provide the data subject in advance with a specific and detailed written privacy notice pursuant to Article 13 GDPR, specifying the purposes, methods, retention periods and exercisable rights. 5.2 Privacy by Design and by Default: The overall architecture of the Company's IT systems, including the ERP management system, PDM (Product Data Management) databases, shared network folders and email systems, must be natively designed and configured so as to minimise the processing of personal data, excluding the collection of information that is not strictly necessary. By default, the Company ensures strong encryption of databases containing personal records, the adoption of pseudonymisation techniques for sensitive files and strict logical isolation of servers in order to prevent unauthorised access, alterations or IT incidents (Data Breaches).

ITALIANO	ENGLISH
Articolo 6 – Criteri Rigidi di Blindatura per le Categorie Particolari di Dati (Art. 9 GDPR) 6.1 Il trattamento delle categorie particolari di dati personali di cui all'Articolo 9 del GDPR (ovvero i dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale e all'orientamento sessuale del lavoratore) è soggetto a restrizioni assolute. Tale trattamento è consentito esclusivamente nei limiti tassativi previsti dalle norme di legge vigenti per l'esecuzione degli obblighi specifici del datore di lavoro in materia di diritto del lavoro, sicurezza sul lavoro e protezione sociale. 6.2 Gestione dei Dati Sanitari e di Idoneità: I dati analitici relativi alla salute dei lavoratori (quali gli esiti delle visite mediche periodiche o straordinarie, le cartelle sanitarie e di rischio professionale, i certificati di malattia, i dati sui tassi di assenteismo per motivi di salute e le registrazioni di infortuni occorsi in produzione) non sono in alcun modo accessibili alla Direzione Aziendale, all'Ufficio Risorse Umane o ai responsabili e capiofficina dei reparti produttivi. Tali record sono custoditi, archiviati ed elaborati in via esclusiva dal Medico Competente nominato dall'Azienda, all'interno di archivi fisici e digitali blindati e protetti da segreto professionale. Alla Direzione Aziendale e all'ufficio HR è comunicato unicamente ed esclusivamente il giudizio finale scritto di idoneità, inidoneità parziale (con relative prescrizioni o limitazioni) o inidoneità totale alla mansione lavorativa specifica. 6.3 Dati di Appartenenza Sindacale: Le informazioni relative alle trattenute sulla busta paga per quote di iscrizione sindacale, all'adesione a sigle dei lavoratori o all'esercizio di diritti e permessi legati alle rappresentanze sindacali aziendali (RSU/RLS) ai sensi del CCNL Metalmeccanico sono trattate con rigorose misure di segregazione logica e controllo degli accessi. È fatto divieto assoluto alla Direzione e a chiunque altro di utilizzare tali dati per scopi valutativi, decisioni sulle carriere, promozioni, assegnazioni di mansioni, premi aziendali o per scopi discriminatori di qualunque natura.	Article 6 – Strict Safeguarding Criteria for Special Categories of Data (Article 9 GDPR) 6.1 Processing of the special categories of personal data referred to in Article 9 GDPR, namely data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as genetic data, biometric data intended to uniquely identify a natural person, data concerning the worker's health or sex life and sexual orientation, is subject to absolute restrictions. Such processing is permitted solely within the mandatory limits laid down by the laws in force for the performance of the employer's specific obligations in the fields of employment law, occupational safety and social protection. 6.2 Management of Health and Fitness Data: Analytical data relating to workers' health, such as the outcomes of periodic or extraordinary medical examinations, health and occupational risk records, sickness certificates, data on absenteeism rates for health reasons and records of injuries occurring in production, are in no way accessible to Company Management, the Human Resources Department or the managers and workshop supervisors of the production departments. Such records are kept, archived and processed exclusively by the Occupational Physician appointed by the Company, within locked-down physical and digital archives protected by professional secrecy. Company Management and the HR Department are informed solely and exclusively of the final written judgement of fitness, partial unfitness, with the relevant prescriptions or limitations, or total unfitness for the specific job duties. 6.3 Trade Union Membership Data: Information relating to payroll deductions for trade union membership fees, membership of workers' organisations or the exercise of rights and leave connected with company trade union representatives (RSU/RLS) pursuant to the Metalworking National Collective Bargaining Agreement is processed with rigorous logical segregation measures and access controls. Management and any other person are absolutely prohibited from using such data for evaluation purposes, career decisions, promotions, assignment of duties, company bonuses or discriminatory purposes of any kind.
Articolo 7 – Trattamento dei Dati dei Candidati nelle Fasi di Selezione 7.1 I curricula vitae e la documentazione associata ricevuti spontaneamente dai candidati o raccolti a seguito di specifiche campagne di ricerca e selezione del personale sono gestiti nel più rigoroso rispetto della Privacy Policy ufficiale della Società. Il trattamento dei dati personali dei candidati deve essere tassativamente limitato alle sole informazioni strettamente necessarie e pertinenti per la valutazione dell'attitudine professionale, delle competenze tecniche e del profilo lavorativo in relazione alla posizione aperta. 7.2 Divieti in Fase di Selezione: È fatto assoluto divieto ai selezionatori, ai consulenti esterni e alla Direzione di richiedere ai candidati informazioni non pertinenti alla mansione professionale, con particolare riferimento alla sfera privata, allo stato civile o familiare, agli orientamenti politici, sindacali o religiosi, alle abitudini personali o a intenzioni presenti o future riguardanti la maternità o la paternità.	Article 7 – Processing of Candidate Data During Recruitment Stages 7.1 Curricula vitae and associated documentation received spontaneously from candidates or collected following specific personnel search and selection campaigns are managed in the strictest compliance with the Company's official Privacy Policy (https://www.tvmolinari.it/privacy-policy/). The processing of candidates' personal data must be strictly limited to information that is absolutely necessary and relevant for assessing professional aptitude, technical skills and work profile in relation to the open position. 7.2 Prohibitions During Recruitment: Recruiters, external consultants and Management are absolutely prohibited from requesting from candidates' information that is not relevant to the professional position, with particular reference to the private sphere, marital or family status, political, trade union or religious views, personal habits or present or future intentions concerning maternity or paternity.

ITALIANO	ENGLISH
7.3 Tempi di Conservazione e Distruzione: I dati personali e i profili dei candidati non idonei o comunque non selezionati al termine del processo di recruiting devono essere permanentemente cancellati dai sistemi informatici (inclusi i client di posta e i server di archiviazione) e distrutti fisicamente tramite dispositivi distruggi-documenti entro e non oltre il termine perentorio di 12 mesi dalla data di ricezione, fatto salvo il caso in cui sia stato acquisito un esplicito, separato e specifico consenso scritto da parte del candidato per una conservazione di più estesa durata.	7.3 Retention Periods and Destruction: The personal data and profiles of candidates who are unsuitable or in any event not selected at the end of the recruitment process must be permanently deleted from IT systems, including email clients and archive servers, and physically destroyed using document shredders no later than the mandatory deadline of 12 months from the date of receipt, except where explicit, separate and specific written consent has been obtained from the candidate for retention for a longer period.
SEZIONE IV: DISPOSIZIONI IN MATERIA DI ETICA ICT, CYBERSECURITY E RESILIENZA (ISO/IEC 27001:2022)	SECTION IV: PROVISIONS ON ICT ETHICS, CYBERSECURITY AND RESILIENCE (ISO/IEC 27001:2022)
Articolo 8 – Integrità dell'Ufficio Tecnico e Protezione della Proprietà Intellettuale	Article 8 – Integrity of the Technical Department and Protection of Intellectual Property
8.1 Custodia Forzata nei Sistemi PDM/ERP: La realizzazione di pezzi speciali, tiranti e viti eseguiti su disegno personalizzato, campionatura o specifica tecnica esclusiva del committente costituisce il nucleo del valore di mercato della Società e richiede la massima protezione informatica della proprietà intellettuale. Tutti i disegni tecnici, i file CAD/CAM, i modelli geometrici 3D e i capitolati inviati in formato digitale dai clienti devono essere archiviati, elaborati e gestiti unicamente ed esclusivamente all'interno del sistema PDM/ERP aziendale protetto.	8.1 Mandatory Safekeeping in PDM/ERP Systems: The production of special parts, tie rods and screws made to customer drawings, samples or exclusive technical specifications constitutes the core of the Company's market value and requires maximum IT protection of intellectual property. All technical drawings, CAD/CAM files, 3D geometric models and specifications sent in digital format by customers must be archived, processed and managed solely and exclusively within the Company's protected PDM/ERP system.
8.2 Misure di Blocco ed Esportazione Indebita: È severamente ed espressamente vietato estrarre, copiare o duplicare file di progettazione e disegni dei clienti tramite supporti di memoria rimovibili USB o hard disk esterni. È vietato caricarli su cloud pubblici non autorizzati o scattare fotografie o acquisire immagini dei monitor delle postazioni di progettazione e sviluppo.	8.2 Blocking Measures and Unlawful Export: It is strictly and expressly prohibited to extract, copy or duplicate design files and customer drawings using removable USB storage media or external hard drives. It is prohibited to upload them to unauthorised public clouds or to take photographs or capture images of monitors at design and development workstations.
8.3 Tracciabilità Totale e Registri Inalterabili (Audit Log): Ogni singola operazione di accesso, visualizzazione, modifica, copia, stampa o scaricamento di un disegno tecnico o di una specifica cliente è tracciata in tempo reale e in modo automatico da registri di log interni al sistema. Tali registri di audit sono strutturati per essere inalterabili, non cancellabili e protetti da crittografia. Essi vengono monitorati e sottoposti ad audit periodici da parte dell'IT Manager e dell'OdV al fine di rilevare tempestivamente comportamenti anomali, tentativi di accesso non autorizzato o download massivi di file non giustificati dalle effettive esigenze lavorative.	8.3 Total Traceability and Immutable Registers (Audit Logs): Every single operation involving access, viewing, modification, copying, printing or downloading of a technical drawing or customer specification is traced in real time and automatically by internal system logs. Such audit logs are structured to be immutable, non-deletable and protected by cryptography. They are monitored and periodically audited by the IT Manager and the Supervisory Body in order to promptly detect anomalous conduct, unauthorised access attempts or mass downloads of files that are not justified by actual work requirements.
Articolo 9 – Gestione delle Identità Informatiche, Autenticazione e Controlli di Rete	Article 9 – Management of IT Identities, Authentication and Network Controls
9.1 Obbligo di Autenticazione a Più Fattori (MFA): L'accesso alla rete informatica aziendale, sia che avvenga dalle postazioni fisiche della sede di Gragnano Trebbiense sia che avvenga da remoto tramite connessioni VPN protette, deve essere presidiato e subordinato all'uso obbligatorio di credenziali personali e univoche associate a sistemi di autenticazione a più fattori (MFA). Le password devono	9.1 Mandatory Multi-Factor Authentication (MFA): Access to the Company IT network, whether from physical workstations at the Gragnano Trebbiense site or remotely through protected VPN connections, must be controlled and conditional upon the mandatory use of personal and unique credentials associated with multi-factor authentication (MFA) systems. Passwords must comply with the complexity criteria established by the

ITALIANO	ENGLISH
rispettare i criteri di complessità stabiliti dalle policy del CdA.	Board of Directors' policies.
9.2 Whitelisting e Divieto di Installazione Software: Tutti i dispositivi informatici di proprietà della Società (inclusi i PC degli uffici, i computer portatili aziendali, i tablet e i terminali industriali integrati a bordo macchina nei reparti produttivi) sono configurati a livello amministrativo per inibire e bloccare l'installazione autonoma di qualsiasi software o applicazione da parte dell'utente. L'utilizzo, l'introduzione o il download di software privi di licenza commerciale, estranei alle attività di produzione o potenzialmente pericolosi (giochi, emulatori, client di file sharing P2P o strumenti di hacking) è tassativamente vietato.	9.2 Whitelisting and Prohibition of Software Installation: All IT devices owned by the Company, including office PCs, company laptops, tablets and industrial terminals integrated on machine tools in the production departments, are configured at administrative level to prevent and block the autonomous installation of any software or application by the user. The use, introduction or download of software without a commercial licence, unrelated to production activities or potentially dangerous (games, emulators, P2P file-sharing clients or hacking tools) is strictly prohibited.
9.3 Divieto Assoluto di Monitoraggio Occulto dei Lavoratori: In rigoroso adempimento delle disposizioni di legge poste dall'Articolo 4 dello Statuto dei Lavoratori (Legge 300/1970) e in perfetta aderenza con le linee guida etiche dello standard ISO 27001, la Società implementa strumenti avanzati di sicurezza informatica della rete e degli endpoint (sistemi EDR/SIEM) configurati al solo ed esclusivo fine di identificare minacce cibernetiche, infezioni da malware, tentativi di intrusione o data breach. Tali strumenti e software di sicurezza sono strutturati in modo da non effettuare, né poter effettuare in alcun modo, alcuna attività di profilazione, sorveglianza continuativa, controllo a distanza o monitoraggio occulto delle performance lavorative, dei ritmi di produzione o della presenza dei dipendenti.	9.3 Absolute Prohibition of Covert Monitoring of Workers: In strict compliance with the statutory provisions laid down by Article 4 of the Workers' Statute (Law 300/1970) and in full adherence to the ethical guidelines of ISO 27001, the Company implements advanced network and endpoint cybersecurity tools (EDR/SIEM systems) configured solely and exclusively for the purpose of identifying cyber threats, malware infections, intrusion attempts or data breaches. Such security tools and software are structured so that they do not carry out, nor can they in any way carry out, any profiling, continuous surveillance, remote control or covert monitoring of employees' work performance, production rates or attendance.
SEZIONE V: PROCEDURA DI SEGNALAZIONE DETTAGLIATA (PIATTAFORMA WHISTLEBLOWING)	SECTION V: DETAILED REPORTING PROCEDURE (WHISTLEBLOWING PLATFORM)
La Società promuove attivamente una cultura aziendale basata sulla trasparenza, sull'etica della responsabilità e sul rifiuto di qualsiasi forma di illegalità od omertà, dotandosi a tal fine di un canale interno di segnalazione strutturato in piena conformità ai requisiti posti dal D.Lgs. 24/2023.	The Company actively promotes a corporate culture based on transparency, the ethics of responsibility and the rejection of any form of illegality or conspiracy of silence, and for this purpose has adopted an internal reporting channel structured in full compliance with the requirements laid down by Legislative Decree 24/2023.
Articolo 10 – Il Canale di Segnalazione Interno "Whistlelink" e Ambito Oggettivo	Article 10 – The "Whistlelink" Internal Reporting Channel and Objective Scope
10.1 Accesso alla Piattaforma Crittografata: TMV Molinari S.r.l. ha istituito, attivato e messo a disposizione di tutti i Destinatari una piattaforma web indipendente, esterna e protetta denominata Whistlelink, il cui punto di accesso è raggiungibile tramite un apposito link posto in chiara evidenza sul portale internet istituzionale. Tale applicazione garantisce, mediante l'utilizzo di protocolli crittografici avanzati a livello di trasporto e di database, l'assoluta e totale riservatezza dell'identità del segnalante (Whistleblower), del contenuto della segnalazione, della documentazione allegata e di tutti i soggetti menzionati o comunque coinvolti nella fattispecie.	10.1 Access to the Encrypted Platform: TMV Molinari S.r.l. has established, activated and made available to all Addressees an independent, external and protected web platform called Whistlelink, access to which is available through a dedicated link clearly displayed on the institutional website. Through the use of advanced cryptographic protocols at transport and database level, the application guarantees the absolute and total confidentiality of the identity of the reporting person (whistleblower), the content of the report, the attached documentation and all persons mentioned or otherwise involved in the matter.
10.2 Ambito Oggettivo delle Segnalazioni: Possono essere oggetto di segnalazione circostanziata tutte le condotte illecite, i reati, le violazioni normative o le fondate e ragionevoli violazioni delle leggi nazionali o dell'Unione Europea, nonché qualsiasi deviazione, elusione o violazione cosciente delle prescrizioni del presente Codice Etico e del Modello di Organizzazione e Gestione 231 della Società. Rientrano obbligatoriamente nell'ambito oggettivo tutelato dalla piattaforma:	10.2 Objective Scope of Reports: All unlawful conduct, offences, regulatory breaches or well-founded and reasonable breaches of national or European Union laws, as well as any deviation from, circumvention of or conscious breach of the provisions of this Code of Ethics and of the Company's Organisation and Management Model pursuant to Legislative Decree 231, may be the subject of a detailed report. The following necessarily fall within the objective scope protected by the platform:

ITALIANO	ENGLISH
- Frodi aziendali, falsificazioni di bilancio, pratiche corruttive, concussione, ricettazione o estorsioni. - Tentativi, sospetti o casi accertati di introduzione di materiali, barre, viti o componenti contraffatti, fraudolenti o sospetti (CFSI - Counterfeit, Fraudulent and Suspect Items) all'interno della linea di fornitura o dei magazzini aziendali. - Gravi e manifeste violazioni delle norme sulla salute e sicurezza nei luoghi di lavoro (Politica HSE), mancata adozione dei DPI obbligatori o casi occulti di inquinamento ambientale, scarichi illeciti o violazione dei parametri di emissione. - Violazioni sistemiche, arbitrarie o continuative delle tutele stabilite dal CCNL Metalmeccanico (quali l'imposizione di turni straordinari non tracciati, la falsificazione dei registri di presenza o condotte vessatorie). - Violazioni delle policy di sicurezza informatica (ISO 27001), furti o tentativi di esportazione di proprietà intellettuale e trattamenti illeciti o non autorizzati di dati sensibili in aperta violazione del GDPR.	- Corporate fraud, falsification of accounts, corrupt practices, extortion by a public official, receiving stolen goods or extortion. - Attempts, suspicions or confirmed cases of the introduction of counterfeit, fraudulent or suspect materials, bars, screws or components (CFSI - Counterfeit, Fraudulent and Suspect Items) into the supply line or Company warehouses. - Serious and evident breaches of occupational health and safety rules (HSE Policy), failure to use mandatory PPE, or concealed cases of environmental pollution, unlawful discharges or breach of emission parameters. - Systemic, arbitrary or continuous breaches of the protections established by the Metalworking National Collective Bargaining Agreement, such as the imposition of unrecorded overtime shifts, falsification of attendance registers or harassing conduct. - Breaches of information security policies (ISO 27001), theft or attempted export of intellectual property and unlawful or unauthorised processing of sensitive data in open breach of the GDPR.
Articolo 11 – Gestione della Segnalazione, Garanzie e Divieto di Ritorsione	Article 11 – Management of Reports, Guarantees and Prohibition of Retaliation
11.1 Competenza Esclusiva dell'Organismo di Vigilanza (OdV): La ricezione, l'esame e la gestione complessiva del canale interno di Whistleblowing sono affidate in via esclusiva all'Organismo di Vigilanza (OdV) della Società. L'OdV è un organo collegiale terzo, dotato per statuto di piena autonomia d'azione, indipendenza finanziaria e specifiche competenze tecniche e giuridiche, incaricato di verificare la fondatezza delle segnalazioni senza subire alcuna ingerenza, condizionamento o controllo da parte del Consiglio di Amministrazione, della direzione o dei soci fondatori. 11.2 Fasi di Elaborazione, Istruttoria e Riscontro Temporale: Il processo di gestione delle segnalazioni è rigorosamente scandito dalle seguenti tempistiche e modalità operative: - Rilascio dell'Avviso di Ricevimento: All'atto dell'invio telematico della segnalazione sulla piattaforma Whistlelink, il sistema genera e rilascia automaticamente al segnalante un codice identificativo univoco e un formale Avviso di Ricevimento entro e non oltre 7 giorni dalla data di ricezione. - Fase Istruttoria Riservata: L'OdV avvia un'istruttoria preliminare e riservata, analizzando i documenti ed effettuando verifiche interne. Qualora sia necessario audire o richiedere informazioni a soggetti interni o esterni all'Azienda, tali audizioni avvengono esclusivamente con modalità idonee a proteggere la riservatezza e l'anonimato del segnalante, escludendo qualsiasi fuga di informazioni.	11.1 Exclusive Competence of the Supervisory Body (OdV): The receipt, examination and overall management of the internal whistleblowing channel are entrusted exclusively to the Company's Supervisory Body (OdV). The OdV is a third-party collegiate body endowed by its statute with full autonomy of action, financial independence and specific technical and legal expertise, tasked with verifying the merits of reports without being subject to any interference, influence or control by the Board of Directors, management or founding shareholders. 11.2 Processing, Investigation and Response Timeframes: The report management process is rigorously governed by the following timeframes and operating methods: - Issuing of the Acknowledgement of Receipt: When a report is submitted electronically on the Whistlelink platform, the system automatically generates and issues to the reporting person a unique identification code and a formal Acknowledgement of Receipt no later than 7 days from the date of receipt. - Confidential Investigation Stage: The OdV commences a preliminary and confidential investigation, analysing documents and carrying out internal checks. Where it is necessary to hear or request information from persons inside or outside the Company, such hearings take place exclusively using methods suitable for protecting the confidentiality and anonymity of the reporting person and excluding any leakage of information.

ITALIANO	ENGLISH
Fornitura del Riscontro Formale: Entro il termine perentorio di 90 giorni calcolati dalla data dell'avviso di ricevimento, l'OdV ha l'obbligo di fornire un riscontro formale, esaustivo e motivato al segnalante, comunicando l'esito dell'istruttoria (archiviazione per infondatezza, accertamento della violazione) e le eventuali misure correttive, sanzionatorie o organizzative adottate o proposte agli organi societari.	Provision of Formal Feedback: Within the mandatory deadline of 90 days calculated from the date of the acknowledgement of receipt, the OdV is obliged to provide formal, comprehensive and reasoned feedback to the reporting person, communicating the outcome of the investigation (filing due to groundlessness, ascertainment of the breach) and any corrective, sanctioning or organisational measures adopted or proposed to the corporate bodies.
11.3 Divieto Assoluto di Ritorsione e Tutele per il Segnalante: La Società vieta, perseguita e sanziona con la massima severità ogni forma di ritorsione, discriminazione, penalizzazione o comportamento vessatorio, sia esso diretto o indiretto, posto in essere a carico del segnalante che abbia effettuato una segnalazione in buona fede. Non è tollerata alcuna misura penalizzante, quali demansionamenti, licenziamenti ritorsivi o discriminatori, trasferimenti ingiustificati di reparto o sede, mutamenti peggiorativi delle condizioni orarie o lavorative, dinieghi di permessi o ferie, o esclusione da percorsi formativi. La violazione del divieto di ritorsione costituisce una violazione disciplinare gravissima e comporta l'immediata applicazione del massimo livello sanzionatorio previsto dal CCNL e dalle leggi vigenti, indipendentemente dal ruolo gerarchico ricoperto dall'autore della ritorsione.	11.3 Absolute Prohibition of Retaliation and Protections for the Reporting Person: The Company prohibits, pursues and sanctions with the utmost severity any form of retaliation, discrimination, penalisation or harassing conduct, whether direct or indirect, carried out against a reporting person who has made a report in good faith. No penalising measure is tolerated, including demotion, retaliatory or discriminatory dismissal, unjustified transfer of department or workplace, detrimental changes to working hours or working conditions, denial of leave or holidays, or exclusion from training pathways. Breach of the prohibition of retaliation constitutes a very serious disciplinary breach and entails the immediate application of the maximum level of sanction provided for by the National Collective Bargaining Agreement and applicable laws, irrespective of the hierarchical role held by the perpetrator of the retaliation.
SEZIONE VI: APPARATO SANZIONATORIO E CONSEGUENZE DELLE VIOLAZIONI	SECTION VI: SANCTIONING SYSTEM AND CONSEQUENCES OF VIOLATIONS
Articolo 12 – Sanzioni per i Lavoratori Dipendenti (CCNL Metalmeccanico)	Article 12 – Sanctions for Employees (Metalworking National Collective Bargaining Agreement)
12.1 L'osservanza scrupolosa di tutte le disposizioni, divieti e protocolli operativi contenuti nel presente Codice Etico, delle regole in materia di prevenzione dei conflitti di interesse, delle norme di blindatura dei dati GDPR e delle policy di cybersecurity ICT aziendali costituisce adempimento formale degli obblighi primari di fedeltà, diligenza e subordinazione del lavoratore subordinato, ai sensi e per gli effetti degli Articoli 2104 e 2105 del Codice Civile.	12.1 Scrupulous compliance with all provisions, prohibitions and operating protocols contained in this Code of Ethics, with the rules on prevention of conflicts of interest, with GDPR data safeguarding rules and with the Company's ICT cybersecurity policies constitutes formal fulfilment of the primary duties of loyalty, diligence and subordination of the employee, pursuant to and for the purposes of Articles 2104 and 2105 of the Italian Civil Code.
12.2 Le infrazioni e le condotte contrarie ai precetti del presente Codice commesse dai lavoratori dipendenti integrano a tutti gli effetti un illecito disciplinare. Esse saranno perseguite e sanzionate dall'Ufficio Risorse Umane secondo un rigoroso principio di proporzionalità in base alla gravità oggettiva del fatto, al grado di colpa o dolo, all'eventuale recidiva e all'entità del danno economico o reputazionale cagionato alla Società. Ogni procedimento disciplinare sarà svolto nel rigido rispetto delle garanzie procedurali stabilite dall'Articolo 7 della Legge 300/1970 (Statuto dei Lavoratori) e dal sistema sanzionatorio del CCNL Metalmeccanico vigente. Le sanzioni applicabili, graduate per gravità, sono:	12.2 Breaches and conduct contrary to the precepts of this Code committed by employees constitute, for all purposes, disciplinary offences. They shall be pursued and sanctioned by the Human Resources Department according to a rigorous principle of proportionality based on the objective seriousness of the act, the degree of negligence or wilful misconduct, any recurrence and the extent of the economic or reputational damage caused to the Company. Every disciplinary procedure shall be conducted in strict compliance with the procedural guarantees established by Article 7 of Law 300/1970 (Workers' Statute) and by the sanctioning system of the Metalworking National Collective Bargaining Agreement in force. The applicable sanctions, graduated by seriousness, are:
Rimprovero verbale: Applicabile in caso di lievi, isolate e del tutto involontarie omissioni o disattenzioni procedurali nell'applicazione delle policy informatiche o delle formalità di registrazione ordinaria.	Verbal reprimand: applicable in the event of minor, isolated and wholly involuntary omissions or procedural oversights in the application of IT policies or ordinary registration formalities.
Ammonizione scritta: Applicabile in presenza di recidiva nelle mancanze minori o nei casi di mancata, ritardata o incompleta disclosure iniziale di una situazione di conflitto di interesse	Written warning: applicable in the event of recurrence of minor breaches or where there has been no initial disclosure, or a late or incomplete initial disclosure, of a potential conflict of interest

ITALIANO	ENGLISH
potenziale che non abbia ancora generato atti negoziali o danni. - Multa non superiore a 4 ore di retribuzione base: Applicabile nei casi di reiterata inosservanza delle procedure interne, violazione delle norme d'uso dei DPI nei reparti di lavorazione o per negligenze accertate nella custodia dei dispositivi IT aziendali. - Sospensione dal servizio e dalla retribuzione fino a un massimo di 10 giorni: Applicabile per violazioni di rilevante gravità, quali il mancato isolamento volontario o la mancata tempestiva segnalazione all'IT Manager di un attacco ransomware in corso, l'utilizzo inappropriato o fuori policy di credenziali di rete, la violazione delle misure di protezione dei dati particolari o sanitari protetti dal GDPR, o la violazione cosciente delle specifiche tecniche di collaudo e laboratorio. - Licenziamento per giustificato motivo soggettivo o per giusta causa: Applicabile per comportamenti caratterizzati da dolo, colpa grave o intenzionalità fraudolenta tali da ledere irrimediabilmente il vincolo fiduciario. Rientrano in questa categoria il compimento di atti ritorsivi contro un whistleblower, l'accettazione di tangenti, regalie non autorizzate o il coinvolgimento attivo in pratiche corruttive o di estorsione.	situation that has not yet generated contractual acts or damage. - Fine not exceeding 4 hours of basic pay: applicable in cases of repeated non-compliance with internal procedures, breach of the rules on use of PPE in processing departments or ascertained negligence in the safekeeping of Company IT devices. - Suspension from work and pay for up to a maximum of 10 days: applicable for breaches of significant seriousness, such as voluntary failure to isolate or promptly report to the IT Manager an ongoing ransomware attack, inappropriate or out-of-policy use of network credentials, breach of measures protecting special category or health data protected by the GDPR, or conscious breach of technical testing and laboratory specifications. - Dismissal for subjective justified reason or for just cause: applicable to conduct characterised by wilful misconduct, gross negligence or fraudulent intent such as to irreparably damage the relationship of trust. This category includes acts of retaliation against a whistleblower, acceptance of bribes, unauthorised gifts or active involvement in corrupt or extortionate practices.
Articolo 13 – Sanzioni per Amministratori e Membri degli Organi di Controllo 13.1 Qualora la violazione delle norme del presente Codice Etico, delle regole sul conflitto di interesse o dei doveri di governance predittiva sia imputabile a uno o più membri del Consiglio di Amministrazione, l'Organismo di Vigilanza (OdV) ha l'obbligo di redigere un'analitica relazione scritta e informare immediatamente l'intero CdA e il Collegio Sindacale. 13.2 Il Collegio Sindacale, ricevuta la notifica dall'OdV, provvederà senza indugio a convocare d'urgenza l'Assemblea dei Soci della Società per deliberare l'adozione delle misure sanzionatorie e di tutela consentite dall'ordinamento, incluse: - La formale censura scritta dell'operato dell'amministratore. - La revoca parziale o totale delle deleghe operative o dei poteri di firma conferiti. - La revoca del mandato consiliare per giusta causa, ai sensi delle norme di legge, senza diritto a indennità risarcitorie. - La promozione e l'esercizio formale dell'azione sociale di responsabilità ai sensi dell'Articolo 2392 del Codice Civile, finalizzata ad ottenere in sede giudiziaria il risarcimento integrale di tutti i danni patrimoniali, economici, commerciali e d'immagine subiti dall'Azienda a causa della condotta illecita dell'amministratore.	Article 13 – Sanctions for Directors and Members of Control Bodies 13.1 Where a breach of the provisions of this Code of Ethics, the rules on conflicts of interest or the duties of predictive governance is attributable to one or more members of the Board of Directors, the Supervisory Body (OdV) is obliged to draw up a detailed written report and immediately inform the entire Board of Directors and the Board of Statutory Auditors. 13.2 Upon receipt of notification from the OdV, the Board of Statutory Auditors shall without delay convene an urgent Shareholders' Meeting of the Company to resolve upon the adoption of the sanctioning and protective measures permitted by law, including: - Formal written censure of the director's conduct. - Partial or total revocation of the operational powers or signing authorities conferred. - Revocation of the directorship for just cause, pursuant to the provisions of law, without entitlement to compensatory indemnities. - Promotion and formal exercise of the corporate liability action pursuant to Article 2392 of the Italian Civil Code, aimed at obtaining in court full compensation for all financial, economic, commercial and reputational damage suffered by the Company as a result of the director's unlawful conduct.



Via dell'Industria, 13-14 – 29010 GRAGNANO TREBBIENSE (PC), ITALY
Tel. +39 0523 575711 – fax +39 0523 592747
P.IVA – C.F. – Registro Imprese 01104300338
Capitale Sociale €300.000,00 i.v.
REA di PC n. 127630
www.tvmolinari.it



CODICE ETICO E DI CONDOTTA INTEGRATO

INTEGRATED ETHIC AND CODE OF CONDUCT

TMV-CECI-01 REV.0 – IT/EN

Pag. 11 / 11

ITALIANO	ENGLISH
Articolo 14 – Clausole Risolute per la Catena di Fornitura, Consulenti e Terzi	Article 14 – Termination Clauses for the Supply Chain, Consultants and Third Parties
14.1 Per tutti i collaboratori esterni, i professionisti incaricati, i consulenti, gli agenti e, in modo tassativo, per tutti i fornitori di materie prime, acciai speciali, semilavorati e servizi di lavorazione esterna, l'osservanza integrale di ogni singolo precetto del presente Codice Etico, il rispetto assoluto della privacy e della sicurezza dei dati, l'assenza di conflitti d'interesse non regolati e la piena conformità alle normative anti-contraffazione CFSI costituiscono condizione essenziale e inviolabili per la nascita, la vigenza e la validità del rapporto d'affari e dei contratti stipulati con la Società.	14.1 For all external collaborators, appointed professionals, consultants, agents and, mandatorily, all suppliers of raw materials, special steels, semi-finished products and external processing services, full compliance with every single precept of this Code of Ethics, absolute respect for privacy and data security, the absence of unmanaged conflicts of interest and full compliance with CFSI anti-counterfeiting regulations constitute an essential and inviolable condition for the creation, continuation and validity of the business relationship and contracts entered into with the Company.
14.2 Ai sensi e per gli effetti dell'Articolo 1456 del Codice civile (Clausola Risolutiva Espressa), l'Azienda inserisce in ogni contratto, lettera d'ordine o accordo di fornitura una specifica clausola che attribuisce alla Società la facoltà e il diritto di attivare la risoluzione immediata e di diritto del contratto a seguito di violazioni accertate del Codice Etico da parte del terzo. L'attivazione della clausola risolutiva espressa determina automaticamente:	14.2 Pursuant to and for the purposes of Article 1456 of the Italian Civil Code (Express Termination Clause), the Company inserts into every contract, purchase order or supply agreement a specific clause granting the Company the power and right to activate immediate termination of the contract by operation of law following ascertained breaches of the Code of Ethics by the third party. Activation of the express termination clause automatically entails:
• L'immediata cessazione di ogni ordine in corso di esecuzione o fornitura aperta, con blocco dei relativi pagamenti.	• The immediate cessation of every order in progress or open supply, with blocking of the relevant payments.
• L'immediata ed automatica cancellazione del fornitore dall'Albo dei Fornitori Qualificati della Società (Vendor List), con divieto assoluto di intrattenere nuove relazioni commerciali per un periodo non inferiore a 60 mesi.	• The immediate and automatic removal of the supplier from the Company's Register of Qualified Suppliers (Vendor List), with an absolute prohibition on entering into new commercial relations for a period of not less than 60 months.
• L'avvio delle azioni legali volte alla richiesta del risarcimento integrale di tutti i danni economici, civili, di fermo produzione e reputazionali subiti dalla Società nei confronti dei propri clienti e dei mercati internazionali.	• The commencement of legal actions seeking full compensation for all economic, civil, production stoppage and reputational damage suffered by the Company vis-à-vis its customers and the international markets.
Il presente testo integrato è depositato presso la Direzione Generale, l'Organismo di Vigilanza ed è reso pubblico e consultabile da chiunque tramite affissione nei reparti e pubblicazione sul portale web della Società.	This integrated text is filed with General Management and the Supervisory Body and is made public and available for consultation by anyone through posting in the departments and publication on the Company's web portal.

TMV MOLINARI SRL Data: 15 luglio 2026

Luca Molinari
CEO & General Manager

TMV MOLINARI S.R.L.
Via dell'Industria, 13 - 0523.575711
29010 Gragnano Trebbiense (Pc)
Partita IVA 01104300338
C.S. € 300.000,00 i.v.