MAGELLANO TECH S.R.L.

P.IVA 16801361003 — Via dei Due Macelli 60, 00187 Roma

CODICE ETICO

Revisione 01 — 14 maggio 2026

Aggiornamento con integrazioni in materia di Intelligenza Artificiale

ISO/IEC 42001:2023 — Reg. (UE) 2024/1689 (AI Act) — L. 132/2025

1. Oggetto, finalità e natura vincolante

Il presente Codice Etico (di seguito, il "Codice") disciplina in modo puntuale e non equivoco i principi, le regole di condotta e gli standard operativi cui devono attenersi Magellano Tech S.r.l. (di seguito, "Magellano" o la "Società") e tutti i soggetti che operano nell'interesse della Società o possono influenzarne l'attività, le decisioni, la reputazione o il rischio.

Il Codice ha quattro finalità principali: (i) orientare le decisioni e i comportamenti quotidiani verso criteri di legalità, integrità e responsabilità; (ii) prevenire condotte improprie o illecite, riducendo i rischi legali, reputazionali e operativi; (iii) definire regole chiare in settori a elevata esposizione (IT, dati, contenuti, AI, marketing, rapporti istituzionali); (iv) costituire il quadro etico di riferimento per il Sistema di Gestione Integrato della Società.

Il Codice non è una dichiarazione di intenti: contiene obblighi di comportamento. Ogni deroga è vietata salvo autorizzazione formale, motivata e tracciata, nei limiti di legge e senza pregiudizio per i principi inderogabili di legalità, correttezza e tutela di terzi.

2. Destinatari e obbligo di conoscenza

Il Codice si applica a: soci, amministratori, dirigenti, dipendenti, collaboratori, consulenti, professionisti esterni, partner, fornitori e a qualunque soggetto terzo che operi in nome o per conto di Magellano o che, di fatto, possa influenzarne attività, decisioni, reputazione o rischio.

Tutti i destinatari hanno l'obbligo di: (i) leggere e comprendere il Codice; (ii) rispettarlo integralmente; (iii) richiedere chiarimenti in caso di dubbio prima di agire; (iv) segnalare tempestivamente violazioni o situazioni di rischio; (v) collaborare in modo leale a verifiche e controlli.

3. Principi inderogabili

Legalità. Ogni attività deve essere svolta nel pieno rispetto delle leggi e delle normative applicabili. Nessun obiettivo economico o commerciale può giustificare la violazione di norme, provvedimenti, autorizzazioni, licenze o obblighi contrattuali.

Integrità sostanziale. È vietato ogni comportamento formalmente corretto ma sostanzialmente scorretto, elusivo o idoneo a ingannare clienti, partner, istituzioni, utenti finali o il mercato. Si

richiede trasparenza reale, non di facciata.

Trasparenza e verificabilità. Le informazioni rilevanti (tecniche, economiche, commerciali, editoriali) devono essere rappresentate in modo veritiero, completo e verificabile. Le decisioni rilevanti devono essere tracciate e riconducibili a responsabilità definite.

Competenza e qualità. Magellano opera con standard tecnici elevati e orientamento alla qualità concreta. Sono vietate promesse non supportate da analisi, metriche, evidenze, test o competenze adeguate.

Riservatezza e tutela dei dati. Le informazioni riservate e i dati personali vanno trattati con rigore, minimizzazione, sicurezza e rispetto delle autorizzazioni. Ogni utilizzo non autorizzato è vietato.

Responsabilità, proporzionalità e supervisione umana. Ogni attività deve essere proporzionata al rischio; quando il rischio aumenta, devono aumentare anche controlli, autorizzazioni, tracciabilità e misure di mitigazione. Questo principio si applica con particolare rigore ai sistemi di intelligenza artificiale, per i quali è sempre garantita una forma di supervisione umana proporzionata al livello di rischio.

4. Obblighi specifici per amministratori, dirigenti e figure apicali

Per "figure apicali" si intendono amministratori, dirigenti, responsabili di funzione e, in generale, chiunque eserciti poteri di rappresentanza, direzione o gestione, anche di fatto.

Obbligo di "tone from the top". Le figure apicali devono essere il primo presidio etico e operativo: il loro comportamento costituisce standard per l'organizzazione. È vietato richiedere, tollerare o incentivare condotte scorrette, anche indirettamente.

Obbligo di organizzazione e controllo. Le figure apicali devono predisporre e mantenere un sistema di procedure coerente con i rischi aziendali: deleghe chiare, segregazione dei compiti ove necessario, livelli autorizzativi, controlli, registrazioni e conservazione documentale. È vietato creare aree di opacità o assenza di controllo.

Obbligo di tracciabilità delle decisioni rilevanti. Ogni decisione significativa deve essere documentata, motivata e approvata secondo i processi interni.

Obbligo di prevenzione dei conflitti di interesse. Le figure apicali devono prevenire conflitti attuali o potenziali. Ogni possibile conflitto deve essere dichiarato prima che produca effetti.

Obbligo di presidio reputazionale e informativo. Le figure apicali devono garantire che comunicazioni, claim commerciali, contenuti editoriali e pubblicitari rispettino criteri di verità, trasparenza e conformità normativa.

Obbligo di presidio cyber e dati. Le figure apicali devono assicurare risorse, competenze e priorità adeguate a sicurezza informatica, continuità operativa e protezione dati.

Obbligo di segnalazione e reazione. Ogni anomalia rilevante deve essere segnalata tempestivamente e gestita con azioni tracciate. Omettere o ritardare è violazione grave.

5. Rapporti con clienti: regole operative non negoziabili

Chiarezza dell'offerta e fattibilità. Ogni offerta deve indicare in modo chiaro scopo, perimetro, deliverable, tempi, vincoli, dipendenze e responsabilità. È vietato vendere servizi senza aver valutato fattibilità tecnica, requisiti, vincoli normativi e risorse.

Contratti coerenti con il lavoro reale. Il contratto deve rappresentare ciò che verrà effettivamente erogato. Sono vietate clausole o promesse "di facciata" non sostenute dall'operatività.

Gestione corretta delle varianti. Ogni variazione di scope, requisiti, tempi o costi deve essere formalizzata e approvata. È vietato "assorbire" varianti rilevanti senza tracciarle.

Tutela di dati e asset del cliente. Accessi, credenziali, dati, codice, documentazione e know-how del cliente devono essere trattati con regole di sicurezza e riservatezza. È vietata ogni riproduzione, riutilizzo o diffusione non autorizzata.

Gestione dei reclami. I reclami vanno trattati con serietà, tempi certi, tracciamento e responsabilità. È vietato negare l'evidenza o scaricare responsabilità senza analisi.

6. Rapporti con fornitori, partner e consulenti

Selezione basata su criteri oggettivi. La scelta di fornitori/partner deve basarsi su competenza, affidabilità, sostenibilità economica, sicurezza, conformità normativa e capacità di erogazione. È vietato selezionare sulla base di favoritismi, utilità personali, pressioni o scambi impropri.

Due diligence proporzionata al rischio. Per fornitori che trattano dati, gestiscono sistemi, producono contenuti o rappresentano la Società verso terzi, è obbligatoria una valutazione preventiva del rischio e l'inserimento di clausole contrattuali adeguate.

Due diligence specifica per fornitori di servizi AI. Per i fornitori di modelli foundation, dataset, servizi di compute e infrastruttura AI, la valutazione preventiva deve includere: (i) dichiarazione di conformità al Regolamento (UE) 2024/1689 (AI Act) e alla L. 132/2025; (ii) presenza di Data Processing Agreement; (iii) misure di sicurezza AI-specifiche; (iv) politiche di data retention e cancellazione; (v) trasparenza sulle fonti dei dati di addestramento.

Pagamenti e condizioni trasparenti. Sono vietati pagamenti non tracciati, condizioni occulte, fatturazioni non coerenti con le prestazioni, triangolazioni sospette e accordi verbali non formalizzati.

Regali, ospitalità e utilità. Sono consentiti solo se: modesti, occasionali, trasparenti, non finalizzati a influenzare decisioni, conformi alle procedure interne. È vietato offrire o accettare utilità che possano anche solo apparire come scambio di favore.

7. Rapporti con Pubblica Amministrazione, Autorità e soggetti pubblici

I rapporti con PA e Autorità devono essere improntati a correttezza assoluta e tracciabilità.

È vietato: (i) promettere, offrire o erogare denaro o utilità indebite, direttamente o indirettamente; (ii) esercitare pressioni improprie; (iii) utilizzare intermediari con finalità illecite; (iv) presentare dichiarazioni o documenti non veritieri; (v) ostacolare controlli.

Ogni interazione con soggetti pubblici rilevante deve essere registrata e gestita da personale autorizzato. Eventuali sponsorizzazioni, contributi, liberalità o iniziative con ricadute su soggetti pubblici devono seguire processi autorizzativi formalizzati e motivati.

8. Regole etiche per le attività digitali della Società (IT, web, marketing, editoria, pubblicità, formazione)

Magellano opera su attività digitali ad alto impatto su utenti, clienti e mercato. Per questa ragione, oltre ai principi generali valgono regole specifiche, qui indicate in forma operativa.

8.1 Consulenza informatica e sviluppo/gestione sistemi

È obbligatorio adottare pratiche professionali adeguate: analisi requisiti, gestione change, versioning, test, ambienti separati, documentazione minima, controllo accessi, backup e ripristino. È vietato introdurre deliberatamente vulnerabilità, backdoor, accessi non autorizzati o usare strumenti illeciti.

8.2 SEO, web marketing, performance e analytics

È vietato utilizzare pratiche ingannevoli, fraudolente o in violazione di norme. Le metriche devono essere presentate in modo fedele e non manipolato, distinguendo risultati organici e a pagamento.

8.3 Editoria elettronica e contenuti

È obbligatorio assicurare: accuratezza ragionevole, verificabilità interna, correttezza delle attribuzioni, rispetto dei diritti d'autore, assenza di plagi, chiarezza su contenuti sponsorizzati. È vietato pubblicare contenuti deliberatamente falsi, fuorvianti o manipolativi.

8.4 Concessionaria di pubblicità e contenuti promozionali

È obbligatorio distinguere in modo chiaro contenuto editoriale e pubblicitario, rispettare regole su trasparenza, comunicazioni commerciali, comparazioni e claim. È vietata qualsiasi comunicazione ingannevole o non dimostrabile.

8.5 Produzione e montaggio video, contenuti multimediali

È obbligatorio rispettare diritti d'immagine, licenze, liberatorie, privacy e copyright. È vietato utilizzare materiale non autorizzato o alterare contenuti in modo da generare falsificazioni dannose.

8.6 Formazione e corsi

È obbligatorio erogare formazione coerente con le competenze dichiarate e con programmi trasparenti. È vietato promettere certificazioni o risultati non garantibili o non previsti.

8-bis. Principi etici per l'uso e lo sviluppo di sistemi di intelligenza artificiale

Magellano sviluppa, fornisce e utilizza sistemi di intelligenza artificiale nell'ambito della propria attività aziendale. In qualità di Provider ai sensi del Regolamento (UE) 2024/1689 (AI Act) per il servizio Concierge24 Genius Medical, e di Deployer per i sistemi AI di terzi utilizzati internamente, la Società adotta i seguenti principi vincolanti.

8-bis.1 Divieto assoluto di pratiche AI vietate

Magellano vieta espressamente — a sé, ai propri dipendenti, collaboratori, consulenti, clienti e fornitori — l'utilizzo dei propri sistemi AI e dei sistemi AI di terzi nell'ambito dell'attività lavorativa per le pratiche vietate dall'art. 5 del Regolamento (UE) 2024/1689, ivi incluse:

(a) tecniche subliminali, manipolative o ingannevoli che distorcano il comportamento di una persona in modo da causare o poter causare un danno significativo;

(b) sfruttamento delle vulnerabilità di gruppi specifici (età, disabilità, condizione sociale o economica) per distorcerne il comportamento;

(c) social scoring: classificazione di persone fisiche basata sul comportamento sociale o su caratteristiche personali con conseguenze pregiudizievoli sproporzionate;

(d) valutazione predittiva del rischio di commissione di reati basata unicamente su profilazione o tratti della personalità;

(e) creazione o espansione di banche dati di riconoscimento facciale mediante scraping non mirato di immagini da internet o da sistemi di videosorveglianza;

(f) riconoscimento delle emozioni in contesti lavorativi e di istruzione, salvo per motivi medici o di sicurezza;

(g) categorizzazione biometrica per dedurre attributi sensibili (razza, opinioni politiche, appartenenza sindacale, convinzioni religiose, orientamento sessuale);

(h) identificazione biometrica remota in tempo reale in spazi accessibili al pubblico (salvo le eccezioni tassative di legge);

(i) generazione di deepfake lesivi ai sensi dell'art. 613-quater c.p.

La violazione di questo divieto costituisce infrazione gravissima e comporta la risoluzione immediata del rapporto con Magellano e l'attivazione di azioni legali.

8-bis.2 Trasparenza e diritto all'informazione

Ogni persona che interagisce con un sistema AI di Magellano deve essere informata di tale interazione, in conformità con l'art. 50 dell'AI Act. Per il servizio Concierge24 Genius Medical, la comunicazione al paziente avviene secondo i testi modello dell'Allegato C e dell'Allegato D del Contratto Master.

8-bis.3 Supervisione umana e responsabilità personale

Nessun sistema AI utilizzato o sviluppato da Magellano opera in regime di completa autonomia decisionale. Per ogni sistema AI è garantita una forma di supervisione umana proporzionata al livello di rischio. Per i sistemi che impattano direttamente persone fisiche è sempre prevista la possibilità di intervento umano.

8-bis.4 Equità, non discriminazione e tutela dei gruppi vulnerabili

I sistemi AI di Magellano non devono produrre output che discriminino persone fisiche sulla base di caratteristiche protette dal diritto dell'Unione europea e dalla Costituzione italiana (sesso, età, etnia, religione, opinioni politiche, condizioni di salute, disabilità, orientamento sessuale, origine sociale). È obbligatorio eseguire test periodici di fairness.

8-bis.5 Privacy by design e protezione dei dati nel contesto AI

I sistemi AI sono progettati secondo i principi di privacy by design e by default. Il trattamento dei dati personali è ridotto al minimo strettamente necessario. Per il servizio Concierge24 Genius Medical vige il principio di cancellazione automatica entro 30 minuti dal completamento della sessione di interazione.

8-bis.6 Valutazione di impatto e gestione del rischio AI

Per ogni sistema AI sviluppato o fornito da Magellano, prima della sua immissione in produzione, è eseguita una valutazione di impatto (AI System Impact Assessment — AIIA) secondo la procedura ISMS-PR-AI-02. La valutazione copre impatti su individui (inclusi gruppi vulnerabili), gruppi protetti e società.

8-bis.7 Uso di sistemi AI di terzi

L'uso di sistemi AI di terzi (LLM, copilot, assistenti generativi) nell'attività lavorativa di Magellano è consentito esclusivamente nel rispetto della Procedura ISMS-PR-AI-05 e della relativa whitelist. È vietato: (i) utilizzare versioni consumer o free tier per attività lavorative; (ii) inserire informazioni riservate, dati personali o codice proprietario in sistemi AI di terzi non approvati; (iii) fare affidamento esclusivo su output AI senza verifica umana.

8-bis.8 Formazione e alfabetizzazione AI

In adempimento dell'art. 4 dell'AI Act, Magellano garantisce un livello adeguato di alfabetizzazione AI per tutto il personale che interagisce con sistemi AI. Il completamento del Modulo M7 "AI Literacy e uso responsabile" (≥3 ore) è condizione necessaria per l'utilizzo strutturato di sistemi AI nell'attività lavorativa.

8-bis.9 Rinvio alla documentazione di sistema

Per il dettaglio operativo delle regole previste dal presente paragrafo si rinvia alla Politica AI (POL-AI-01), alla Procedura per l'Uso Responsabile dei Sistemi AI (ISMS-PR-AI-05), alla Procedura AIIA (ISMS-PR-AI-02), all'Organigramma Ruoli AI (ISMS-MOD-AI-04C) e alla Dichiarazione di Presa Visione (ISMS-MOD-AI-06).

9. Rischi reputazionali: prevenzione, regole e gestione delle crisi

Per "rischio reputazionale" si intende qualsiasi evento, contenuto, comportamento o omissione che possa compromettere la fiducia di clienti, partner, istituzioni, utenti finali o del pubblico nei confronti di Magellano.

Fonti tipiche di rischio reputazionale per una società digitale

In particolare, generano rischio elevato: (i) claim commerciali non dimostrabili o promesse eccessive; (ii) contenuti editoriali fuorvianti o percepiti come manipolativi; (iii) commistione non trasparente tra informazione e pubblicità; (iv) gestione inadeguata di dati personali o incidenti di sicurezza; (v) uso non trasparente o discriminatorio di sistemi AI; (vi) output AI offensivi, falsi o lesivi prodotti da sistemi di Magellano.

Regole preventive obbligatorie

(1) Ogni messaggio esterno rilevante deve essere coerente con fatti, contratti e capacità operative. (2) Ogni contenuto promozionale deve essere chiaramente identificabile e distinguibile. (3) Per i contenuti che possono influenzare decisioni rilevanti di terzi è necessaria verifica interna preventiva.

Social media e comportamento pubblico

Chi parla a nome della Società o è riconoscibile come rappresentante deve mantenere condotta professionale e prudente: è vietato divulgare informazioni riservate, attaccare clienti/partner, alimentare polemiche che possano ricadere su Magellano, diffondere contenuti non verificati.

Gestione delle crisi reputazionali

Quando si verifica un evento potenzialmente reputazionale, è obbligatorio: (i) attivare un canale interno di escalation; (ii) raccogliere fatti e prove; (iii) congelare modifiche non tracciate; (iv) definire una risposta condivisa; (v) comunicare solo dopo verifica dei fatti.

10. Rischi informatici e protezione delle informazioni: standard minimi obbligatori

Per "rischio informatico" si intende qualunque minaccia a confidenzialità, integrità e disponibilità di dati e sistemi (es. accessi abusivi, malware, ransomware, data leak, interruzioni di servizio, manipolazioni di contenuti, frodi digitali).

Ai rischi informatici tradizionali si aggiungono le minacce specifiche dei sistemi di intelligenza artificiale, che includono: prompt injection, data poisoning, model inversion, adversarial examples, supply chain attacks sui modelli, e abuso di API AI. Tali minacce richiedono misure di mitigazione dedicate.

Principi di sicurezza

La sicurezza è responsabilità di tutti. Si applicano almeno: minimizzazione degli accessi, principio del minimo privilegio, separazione ambienti, hardening, patching, logging, backup, piani di continuità.

Gestione degli accessi e credenziali

È obbligatorio: (i) utilizzare credenziali uniche; (ii) proteggere password e token; (iii) abilitare, dove possibile, autenticazione forte; (iv) revocare immediatamente gli accessi alla cessazione di incarichi; (v) vietare condivisioni informali di credenziali.

Sicurezza operativa e supply chain digitale

L'uso di fornitori IT, cloud, tool di terze parti, plugin, componenti software e servizi esterni deve essere valutato per rischio e conformità. È vietato introdurre componenti non autorizzati in ambienti produttivi. Devono esistere criteri minimi per aggiornamenti, patch e gestione vulnerabilità.

Protezione dati e documenti

È obbligatorio classificare e proteggere le informazioni in base a sensibilità. È vietato trasferire dati su canali non autorizzati o archiviare informazioni riservate su dispositivi o account personali senza autorizzazione.

Incident management

Qualsiasi incidente o sospetto incidente deve essere segnalato immediatamente secondo le procedure. È obbligatorio conservare evidenze tecniche, evitare interventi improvvisati che cancellino tracce e attivare i canali di escalation.

Formazione

La Società deve garantire formazione periodica su rischi cyber e data protection; i destinatari devono partecipare e applicare le regole. La negligenza ripetuta su aspetti di sicurezza costituisce violazione grave.

11. Risorse umane, ambiente di lavoro e regole di condotta interna

Magellano promuove un ambiente di lavoro basato su rispetto, collaborazione, responsabilità e merito.

È vietata ogni forma di discriminazione, molestia, intimidazione o comportamento lesivo della dignità personale. Il dissenso professionale è ammesso e gestito con metodi civili e tracciabili. La Società tutela la salute e sicurezza sul lavoro, richiedendo a tutti comportamenti prudenti e conformi alle norme.

Ogni destinatario deve evitare comportamenti che compromettano la qualità del lavoro o la fiducia reciproca (es. falsificazione di timesheet, alterazione report, appropriazione indebita di materiali, sabotaggi, abuso di permessi).

12. Utilizzo dei beni aziendali e tutela del patrimonio

I beni materiali e immateriali (hardware, software, licenze, account, archivi, documentazione, know-how, database, codici, contenuti) devono essere usati esclusivamente per finalità professionali e nel rispetto delle autorizzazioni.

È vietato: (i) installare software non autorizzato; (ii) utilizzare risorse aziendali per attività personali ad alto rischio o illegittime; (iii) esportare dati o codici senza titolo; (iv) utilizzare licenze in modo non conforme; (v) compromettere integrità di sistemi.

13. Segnalazioni, tutela del segnalante e controlli

Magellano promuove la segnalazione responsabile di violazioni o rischi, garantendo riservatezza, tutela del segnalante e divieto assoluto di ritorsioni.

Le segnalazioni devono essere circostanziate e in buona fede. Sono vietate segnalazioni calunniose o strumentali. La Società si impegna a valutare le segnalazioni con tempestività, a documentare le verifiche e ad adottare misure correttive.

I canali di segnalazione disponibili includono: la piattaforma whistleblowing (magellanotech.it/whistleblowing/, ex D.Lgs. 24/2023) e il canale etico AI (ai-ethics@magellanotech.it).

14. Violazioni e conseguenze

La violazione del Codice comporta conseguenze proporzionate alla gravità: richiami, misure disciplinari, risoluzione del rapporto, azioni di rivalsa e, quando necessario, segnalazione alle autorità competenti.

Sono considerate violazioni gravi: corruzione o tentativi, frodi, falsificazioni documentali, violazioni intenzionali di sicurezza, uso illecito di dati, occultamento di incidenti, conflitti di interesse non

dichiarati, manipolazioni comunicative ingannevoli, utilizzo di sistemi AI per pratiche vietate dall'art. 5 AI Act.

15. Adozione, diffusione e aggiornamento

Il Codice è approvato dall'organo amministrativo, diffuso a tutti i destinatari e aggiornato quando mutano normative, organizzazione o rischi. La Società garantisce strumenti di informazione e formazione per assicurare applicazione effettiva.

Il presente Codice è pubblicato sul sito istituzionale magellanotech.it. La presa visione del Codice è documentata nel modulo ISMS-MOD-30 (Presa Visione Politiche SGI) e costituisce condizione per l'accesso ai sistemi aziendali.
