[AMIU S.p.A.]

POLICY INTERNA PER L'UTILIZZO ETICO, SICURO E CONFORME DEI SISTEMI DI INTELLIGENZA ARTIFICIALE GENERATIVA

Regolamento operativo per dipendenti, collaboratori, RUP e dirigenti (Aggiornato al D.Lgs. 160/2026 e D.Lgs. 179/2026)

Sommario

ART. 1 — FINALITÀ, OGGETTO E AMBITO DI APPLICAZIONE 2
ART. 2 — PRINCIPI FONDAMENTALI E GOVERNANCE 2
ART. 3 — DIVIETO DI «SHADOW AI» E AUTORIZZAZIONE PREVENTIVA (WHITELISTING) 2
ART. 4 — REGOLE DI SICUREZZA NEL PROMPTING E PROTEZIONE DEI DATI 3
ART. 5 — PROTOCOLLO DI SORVEGLIANZA UMANA («HUMAN-IN-THE-LOOP») 3
ART. 6 — TUTELA DEI LAVORATORI E DIVIETO DI MONITORAGGIO ALGORITMICO 4
ART. 7 — FORMAZIONE OBBLIGATORIA (AI LITERACY) E AGGIORNAMENTO DVR 4
ART. 8 — SISTEMA DISCIPLINARE E CONTROLLI 4
ART. 9 — DISPOSIZIONI FINALI E ENTRATA IN VIGORE 4

ART. 1 — FINALITÀ, OGGETTO E AMBITO DI APPLICAZIONE

1. Il presente Regolamento (di seguito «AI Policy») disciplina l'utilizzo dei sistemi di Intelligenza Artificiale (IA), con particolare riferimento ai modelli di IA generativa (es. LLM, assistenti di scrittura, generatori di immagini, codice e sintesi documentale), da parte di tutti i dipendenti, dirigenti, responsabili di procedimento (RUP), consulenti e collaboratori a qualsiasi titolo di AMIU S.p.A. (di seguito «l'Ente»). Restano esclusi gli usi personali al di fuori dell'orario di lavoro e dei dispositivi aziendali.

2. La presente Policy recepisce e dà attuazione al Regolamento (UE) 2024/1689 (AI Act), alla Legge 23 settembre 2025, n. 132, al D.Lgs. 9 settembre 2026, n. 160 (introduzione dell'art. 25-vicies nel D.Lgs. 231/2001 e reati ex artt. 437-bis e 612-quater c.p.), al D.Lgs. 7 ottobre 2026, n. 179 in materia di sicurezza sul lavoro e tutela del rapporto di lavoro, nonché alle linee guida dell'Agenzia per l'Italia Digitale (AgID) e dell'Agenzia per la Cybersicurezza Nazionale (ACN).

3. L'obiettivo primario della Policy è coniugare l'innovazione tecnologica e l'efficienza amministrativa/aziendale con la tutela rigorosa dei diritti fondamentali dei cittadini e dei lavoratori, la cybersicurezza, la protezione dei dati personali (GDPR) e la prevenzione dei reati presupposto della responsabilità amministrativa degli enti.

ART. 2 — PRINCIPI FONDAMENTALI E GOVERNANCE

L'utilizzo di qualsiasi sistema di IA all'interno dell'Ente si fonda sui seguenti principi inderogabili:

a) Principio di Antropocentricità e Strumentalità Algoritmica: L'intelligenza artificiale ha natura esclusivamente strumentale e di supporto all'attività istruttoria umana. È fatto divieto di attribuire a sistemi algoritmici la titolarità o la decisione autonoma di procedimenti amministrativi, atti d'ufficio o valutazioni sul personale. La decisione finale spetta sempre e comunque alla persona fisica (Amministratore Unico, dirigente, RUP o funzionario/dipendente), che ne assume piena ed esclusiva responsabilità ai sensi della L. 241/1990 e delle normative vigenti.
b) Principio di Trasparenza e Spiegabilità: L'utilizzo di strumenti di supporto basati su IA nell'istruttoria di atti, gare pubbliche o procedimenti deve essere chiaramente tracciato. Gli output generati devono essere verificabili, spiegabili e immuni da opacità tecnologica («effetto scatola nera»).
c) Principio di Non Discriminazione e Correttezza: I sistemi IA impiegati non devono generare discriminazioni basate su sesso, razza, origine etnica, religione, opinioni politiche, orientamento sessuale o condizioni sociali ed economiche.

ART. 3 — DIVIETO DI «SHADOW AI» E AUTORIZZAZIONE PREVENTIVA (WHITELISTING)

1. È fatto divieto assoluto a tutti i dipendenti di utilizzare strumenti, piattaforme, estensioni per browser o applicazioni di Intelligenza Artificiale (inclusi strumenti di IA generativa gratuiti, freemium o di libero accesso su internet) che non siano stati espressamente autorizzati dall'Ente («Divieto di Shadow AI»).

2. L'Ente adotta un regime di «Whitelisting». L'elenco dei software di IA approvati, testati e contrattualizzati in ambiente enterprise sicuro è pubblicato e costantemente aggiornato nel «Registro Interno dei Sistemi di IA», consultabile sulla intranet aziendale a cura del Responsabile IIT (RIT).

3. Qualora un dipendente o dirigente ravvisi la necessità di introdurre un nuovo applicativo di IA, deve inoltrare formale richiesta scritta al Comitato di Valutazione IA (composto da RIT, DPO e CISO). Nessun software IA può essere installato o impiegato senza il preventivo «Permesso all'Utilizzo» rilasciato per iscritto.

ATTENZIONE — SANZIONI DISCIPLINARI E PENALI PER L'USO DI SHADOW AI

L'utilizzo non autorizzato di IA («Shadow AI») o l'immissione di dati riservati e personali in piattaforme pubbliche non contrattualizzate espone l'operatore a procedimenti disciplinari severi (fino al licenziamento per giusta causa), nonché a responsabilità penali personali per violazione del segreto d'ufficio (art. 326 c.p.), trattamento illecito di dati (art. 167 GDPR) e violazione degli obblighi di sicurezza ex art. 437-bis c.p., che comportano altresì la contestazione della responsabilità amministrativa dell'Ente ex D.Lgs. 231/2001.

ART. 4 — REGOLE DI SICUREZZA NEL PROMPTING E PROTEZIONE DEI DATI

Nell'interazione con i sistemi di IA autorizzati in ambiente enterprise, i dipendenti devono attenersi rigorosamente alle seguenti regole di prompting e tutela informativa:

a) Divieto di immissione di dati personali in chiaro: È tassativamente vietato inserire nei prompt nomi, cognomi, codici fiscali, indirizzi, numeri di telefono o qualsiasi dato idoneo a identificare direttamente o indirettamente interessati, cittadini, dipendenti o terzi, salvo l'utilizzo di dati preventivamente anonimizzati o pseudonimizzati secondo l'utilizzo di apposito software approvato dal Comitato di Valutazione IA e/o le istruzioni del DPO.
b) Divieto di immissione di segreti d'ufficio, dati riservati o bozze di atti sensibili: È vietato inserire nei sistemi IA informazioni coperti da segreto d'ufficio, strategie aziendali riservate, bozze di provvedimenti amministrativi non ancora pubblicati, offerte economiche o dati relativi a gare d'appalto in corso, se non all'interno di ambienti cloud isolati e contrattualmente blindati («Zero Data Retention Agreements»).
c) Obbligo di verifica delle «Allucinazioni Algoritmiche»: I dipendenti prendono atto che i sistemi di IA generativa operano su base probabilistica e possono produrre informazioni false, imprecise o inventate («allucinazioni»). Ogni testo, dato o riferimento normativo generato dall'IA deve essere sempre verificato con diligenza professionale prima di essere utilizzato in atti ufficiali.

ART. 5 — PROTOCOLLO DI SORVEGLIANZA UMANA («HUMAN-IN-THE-LOOP»)

1. L'output generato da un sistema di IA costituisce esclusivamente una bozza o un materiale istruttorio di supporto e non riveste in alcun modo carattere vincolante o provvedimentale.

2. Ciascun Dirigente, Responsabile di Area, RUP o dipendente è nominato «Garante della Sorveglianza Umana» per i procedimenti di propria competenza. Egli ha l'obbligo di:

• Verificare analiticamente la correttezza, la completezza e la fondatezza di ogni elaborato prodotto con il supporto dell'IA.
• Validare e sottoscrivere personalmente il provvedimento o l'atto finale, assumendosi la totale paternità intellettuale e giuridica dell'atto.
• Attivare immediatamente la funzione di blocco o sospensione del sistema («stop button») e segnalare al CISO e all'OdV qualsiasi anomalia, bias discriminatorio o malfunzionamento critico.

ART. 6 — TUTELA DEI LAVORATORI E DIVIETO DI MONITORAGGIO ALGORITMICO

1. Ai sensi dell'art. 41 del D.Lgs. 7 ottobre 2026, n. 179, è fatto divieto assoluto di adottare decisioni o provvedimenti incidenti sul rapporto di lavoro dei dipendenti (ivi inclusi procedimenti disciplinari, valutazioni della performance, progressioni economiche o mansioni) basati unicamente su processi decisionali automatizzati o sistemi di IA privi di significativa supervisione umana.

2. L'utilizzo di sistemi di IA finalizzati al monitoraggio dell'attività lavorativa rispetta integralmente lo Statuto dei Lavoratori (art. 4 L. 300/1970) e le procedure di preventiva informativa e confronto sindacale.

ART. 7 — FORMAZIONE OBBLIGATORIA (AI LITERACY) E AGGIORNAMENTO DVR

1. Ai sensi dell'art. 4 del Reg. UE 2024/1689 e dell'art. 42 del D.Lgs. 179/2026, l'Ente garantisce a tutti i dipendenti, dirigenti e RUP percorsi di formazione obbligatoria e periodica in materia di alfabetizzazione sull'intelligenza artificiale («AI Literacy»).

2. Il Datore di Lavoro, di concerto con l'RSPP e il Medico Competente, provvede ad aggiornare il Documento di Valutazione dei Rischi (DVR ex D.Lgs. 81/2008) includendo la valutazione dei rischi psicosociali, ergonomici e di stress correlati all'impiego di strumenti di IA.

ART. 8 — SISTEMA DISCIPLINARE E CONTROLLI

1. La violazione delle disposizioni contenute nella presente AI Policy, l'uso non autorizzato di strumenti di IA («Shadow AI»), la violazione delle regole di prompting o l'omessa supervisione umana costituiscono illecito disciplinare e violazione del Codice di Comportamento dell'Ente.

2. Tali condotte comportano l'applicazione delle sanzioni disciplinari previste dal CCNL di comparto e dal Sistema Disciplinare integrato nel Modello 231, proporzionate alla gravità della violazione, ferma restando ogni altra responsabilità civile, penale o erariale.

ART. 9 — DISPOSIZIONI FINALI E ENTRATA IN VIGORE

1. La presente AI Policy entra in vigore il giorno successivo alla sua pubblicazione nella intranet istituzionale ed è portata a conoscenza di tutto il personale mediante comunicazione circolare e/o consegna a mani/notifica telematica e/o affissione in bacheche aziendali.

2. La Policy è soggetta a revisione periodica, ovvero tempestivamente in caso di modifiche normative o evoluzioni tecnologiche rilevanti.