REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	Determina dell'Amministratore Unico del 9.02.2026	ADOZIONE

POLITICA SULL'UTILIZZO DELL'INTELLIGENZA ARTIFICIALE

GETOPEN S.R.L.

SOMMARIO

SOMMARIO 2

1. DEFINIZIONI E AMBITO NORMATIVO

IA: è il ramo dell'informatica che studia e sviluppa sistemi capaci di svolgere compiti che normalmente richiederebbero l'intelligenza umana, consentendo di migliorarne le prestazioni.

Questo sistema, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali;

MACHINE LEARNING: è un processo di apprendimento automatico effettuato da parte dell'IA che impara dai dati forniti riuscendo a ottenere output (ovvero previsioni, contenuti, raccomandazioni o decisioni), ricavandone inoltre modelli e algoritmi atti a modificare nel continuo in modalità adattiva le piattaforme che li utilizzano;

CHATBOT DI IA: è un sistema software che utilizza tecniche di IA, in particolare di elaborazione del linguaggio naturale (NLP) e machine learning, per comprendere, interpretare e generare risposte in linguaggio umano durante una conversazione con un utente.

ROBOT PROCESS AUTOMATION: è una tecnologia che utilizza software ("robot") per automatizzare attività operative ripetitive e basate su regole, replicando le azioni che un operatore umano svolgerebbe su sistemi digitali (ad esempio inserire dati, copiare informazioni, compilare moduli, eseguire controlli). In particolare, le tecnologie di RPA sostituiscono quindi l'intervento umano in questi compiti, consentendo di risparmiare tempo, ridurre gli errori e liberare gli addetti per attività a maggior valore aggiunto.

DATI PERSONALI: qualsiasi informazione riguardante una persona fisica identificata o identificabile, ai sensi del GDPR.

DATI RISERVATI/CONFIDENZIALI: informazioni non pubbliche relative alla Società, ai suoi clienti, fornitori o partner (es. documenti interni, codice sorgente, informazioni finanziarie, strategie di business).

2 SCOPO DELLA POLICY IA

Lo scopo della presente policy sull'Intelligenza Artificiale (IA) è quello di fissare regole chiare e condivise su come l'IA viene usata, da chi e con quali limiti, per massimizzare i benefici riducendo rischi e problemi, mediante una corretta definizione di quali dati si possono usare, per quali finalità e con quali strumenti.
Inoltre, qualora la società dovesse consentire l'uso di applicazioni di IA, le stesse saranno autorizzate solo se conformi alle normative vigenti, nazionali ed europee, e che rispettino i principi etici fondamentali in modo da garantire un utilizzo profittevole dell'IA non andando incontro a rischi reputazionali e di non compliance.

3 AUTORIZZAZIONE ALL'USO DI APPLICAZIONI DI INTELLIGENZA ARTIFICIALE

L'utilizzo di applicazioni, strumenti, piattaforme o sistemi basati su Intelligenza Artificiale, inclusi – a titolo esemplificativo e non esaustivo – sistemi di generazione automatica di testi, immagini, codice, analisi di dati o supporto decisionale, è espressamente riservato all'Amministratore Unico della Società.
È fatto divieto a dipendenti e a tutti coloro che operano in nome e per conto della Società, di utilizzare, direttamente o indirettamente, applicazioni di Intelligenza Artificiale per finalità lavorative, aziendali o comunque riconducibili all'attività della Società, in assenza di preventiva autorizzazione scritta dell'Amministratore Unico.
Ogni utilizzo non autorizzato di strumenti di Intelligenza Artificiale costituisce violazione della presente Policy e potrà comportare l'adozione dei provvedimenti previsti dalla normativa vigente, dai contratti applicabili e dai regolamenti interni, fatto salvo il risarcimento di eventuali danni. In particolare, il divieto è finalizzato, alla tutela dei dati personali, delle informazioni riservate e del patrimonio informativo della Società.
Per l'Amministratore Unico è consentito l'utilizzo di Claude di Anthropic e Gemini di Google che sono degli assistenti virtuali basati sull'intelligenza artificiale.

L'utilizzo di Claude di Anthropic e di Gemini di Google da parte dell'Amministratore Unico dovrà avvenire nel rispetto delle condizioni contrattuali applicabili e delle misure di protezione dei dati previste dalla versione del servizio utilizzata, privilegiando, ove possibile, soluzioni che offrano adeguate garanzie in termini di protezione dei dati, limitazione dell'uso dei contenuti per finalità di addestramento e disponibilità di specifici accordi sul trattamento dei dati.

Resta inteso che la Società mantiene il ruolo di titolare del trattamento per ogni trattamento di dati personali effettuato mediante strumenti di Intelligenza Artificiale, e che l'utilizzo di tali strumenti non esonera la Società dalle responsabilità previste dalla normativa vigente in materia di protezione dei dati personali.

In ordine alla privacy aziendale, sia Claude Anthropic che Gemini di Google offrono soluzioni avanzate per la privacy aziendale, garantendo che, per i piani a pagamento (Team/Enterprise), i dati aziendali non vengano utilizzati per addestrare i loro modelli, ma le modalità di gestione dei dati, la residenza e le integrazioni variano.

ANTHROPIC si impegna a rispettare rigorosi standard di privacy per assicurare che i dati degli utenti siano trattati in modo sicuro e trasparente. Questo include l'implementazione di misure di sicurezza avanzate, come la crittografia dei dati e l'accesso controllato, per prevenire accessi non autorizzati e garantire la conformità alle normative vigenti, come il GDPR.

Inoltre, Anthropic adotta pratiche di privacy by design, integrando la protezione dei dati fin dalle prime fasi dello sviluppo dei modelli AI. Questo approccio proattivo aiuta a minimizzare i rischi di violazione della privacy e a costruire la fiducia degli utenti.

Un altro aspetto importante è la trasparenza. Anthropic fornisce informazioni chiare su come i dati vengono utilizzati e offre agli utenti il controllo sui propri dati, consentendo loro di gestire le proprie preferenze di privacy.

In sintesi, la privacy nei modelli AI di Anthropic è un elemento chiave che combina sicurezza, trasparenza e conformità normativa per offrire un'esperienza utente sicura e affidabile.

Anthropic implementa misure avanzate per proteggere i dati degli utenti. Queste misure includono:

CRITTOGRAFIA DEI DATI: Tutti i dati sensibili sono crittografati sia in transito che a riposo, utilizzando standard di crittografia avanzati.

ACCESSO LIMITATO: Solo il personale autorizzato può accedere ai dati, e tutti gli accessi sono monitorati e registrati.

ANONIMIZZAZIONE: I dati personali vengono anonimi prima di essere utilizzati per l'addestramento dei modelli, per garantire che non siano tracciabili a individui specifici.

Gemini AI è un modello di intelligenza artificiale sviluppato da Google, progettato per offrire soluzioni avanzate in vari settori, tra cui la ricerca, la generazione di testo, e la comprensione del linguaggio naturale. Questo modello è stato creato per essere altamente efficiente e capace di gestire compiti complessi con precisione e velocità. Gemini AI è stato addestrato su un vasto corpus di dati provenienti da diverse fonti, permettendogli di comprendere e generare testo in modo coerente e contestualmente appropriato. Il modello supporta anche funzionalità avanzate come la generazione di immagini e la traduzione multilingua, rendendolo uno strumento versatile per diverse applicazioni.

Gemini AI si impegna a garantire la privacy e la sicurezza dei dati degli utenti con soluzioni avanzate e trasparenti. La piattaforma utilizza tecnologie di crittografia avanzata per proteggere le informazioni sensibili durante la trasmissione e lo storage. Inoltre, Gemini AI adotta misure rigorose per la gestione dei dati, inclusa la minimizzazione dei dati raccolti e l'accesso limitato solo a personale autorizzato.

La conformità alle normative sulla privacy è un aspetto fondamentale per Gemini AI. La piattaforma è progettata per essere conforme alle normative internazionali più stringenti, come il GDPR e il CCPA, assicurando che i dati degli utenti siano

trattati in modo sicuro e rispettoso. Gemini AI offre anche strumenti per consentire agli utenti di controllare e gestire i propri dati, inclusa la possibilità di richiedere l'eliminazione dei dati personali.

La trasparenza è un altro pilastro della gestione della privacy da parte di Gemini AI. La piattaforma fornisce documenti chiari e dettagliati sulla politica sulla privacy, inclusi i tipi di dati raccolti, lo scopo del trattamento e le misure di sicurezza adottate. Inoltre, Gemini AI mantiene una documentazione aggiornata su eventuali aggiornamenti alle politiche sulla privacy e sulle misure di sicurezza.

Dunque, i dati non vengono esaminati da persone né utilizzati per l'addestramento di modelli di AI generativa al di fuori del tuo dominio senza autorizzazione.

Gemini è dotato di difese contro gli attacchi di prompt injection indiretti e di controlli DLP granulari per aiutare a proteggere i contenuti sensibili.

4 AMBITO NORMATIVO

4.1 RIFERIMENTI NORMATIVI INTERNAZIONALI

La presente policy si conforma al Regolamento UE 2024/1689 sull'IA, che stabilisce requisiti per la sicurezza, affidabilità e trasparenza dei sistemi di IA, integrando, altresì, i principi etici promossi dalle linee guida OCSE e UNESCO.

Il Regolamento UE 2024/1689 si basa su regole armonizzate per lo sviluppo e l'immissione sul mercato di sistemi sull'IA nell'Unione Europea con l'obiettivo di promuovere un'IA antropocentrica e affidabile, proteggendo al contempo la salute, la sicurezza e i diritti fondamentali dei cittadini europei. Tale norma, che sfrutta un risk based approach, si applica a fornitori, distributori e utilizzatori di sistemi IA garantendo un suo uso etico e vietando alcune pratiche scorrette come la manipolazione subliminale, lo sfruttamento delle vulnerabilità delle persone, il social scoring, la valutazione del rischio basata sulla profilazione e l'uso di sistemi di IA per provocare emozioni sul luogo di lavoro.

Inoltre, il citato regolamento prevede anche la promozione dell'utilizzo etico dell'IA, stabilisce sanzioni in caso di uso scorretto e viene esaminato periodicamente dalla Commissione Europea per garantirne la sua adeguatezza e attualità.

LE LINEE GUIDA OCSE garantiscono il rispetto di alcuni principi etici fondamentali, in particolare:

I) CRESCITA INCLUSIVA, SVILUPPO SOSTENIBILE E BENESSERE: le parti interessate devono impegnarsi in modo proattivo a promuovere la gestione responsabile di una IA affidabile, al fine di aumentare le capacità umane, la creatività, l'inclusione e ridurre le disuguaglianze, incentivando la crescita economica e la sostenibilità ambientale;

II) RISPETTO PER LO STATO DI DIRITTO, I DIRITTI UMANI E I VALORI DEMOCRATICI: A tal fine, i vari operatori dovrebbero implementare meccanismi e salvaguardie, come la sorveglianza umana, anche per affrontare i rischi derivanti da utilizzi al di fuori dello scopo previsto, o da un uso improprio (intenzionale o meno). Tra i valori da rispettare rientrano, tra gli altri, l'uguaglianza e la non discriminazione, la libertà, la dignità e l'autonomia umana, la tutela della vita privata e la protezione dei dati personali, la diversità e l'equità, la giustizia sociale e la tutela dei diritti dei lavoratori promossa a livello internazionale;

III) TRASPARENZA: è necessario garantire la trasparenza della comunicazione in relazione ai sistemi di IA;

IV) SICUREZZA E AFFIDABILITÀ: le applicazioni di IA dovrebbero essere sicure e affidabili in condizioni di normale utilizzo, uso prevedibile o uso improprio, prevedendo, altresì, sistemi finalizzati ad annullare, riparare o disattivare i sistemi nell'ipotesi in cui gli stessi abbiano cagionato dei danni o causano danni;

L'UNESCO PROPONE DELLE LINEE GUIDA, in particolare**:**

I) PRINCIPI ETICI FONDAMENTALI: rispetto dei diritti umani, inclusività, sostenibilità ambientale, privacy e protezione dei dati e trasparenza. A tal fine è necessario assicurare il rispetto delle disposizioni a protezione della privacy, nonché promuovere l'equità e l'inclusione, garantendo la formazione sull'uso dell'IA e favorendo la diversità di idee e l'inclusione.

4.2 RIFERIMENTI NORMATIVI NAZIONALI

La presente policy è conforme:

- al Regolamento UE 2024/1689 e al Regolamento UE 2016/679 (GDPR), i quali assicurano il rispetto dei principi etici base, dei diritti dell'uomo e dei lavoratori;
- alla legge 132/2025, con la quale l'Italia ha definito i principi e regole per lo sviluppo e l'utilizzo dell'intelligenza artificiale in tutti i settori strategici del Paese, dalla sanità alla giustizia, dalla pubblica amministrazione al lavoro

5. PRINCIPI GENERALI

5.1 ETICA E TRASPARENZA

GETOPEN si impegna a garantire che tutte le applicazioni di IA che verranno utilizzate dalla società dovranno essere utilizzate in modo etico e trasparente, rispettando i diritti umani e promuovendo la fiducia dei clienti.

L'utilizzo di soluzioni di IA deve: **1.** garantire la trasparenza comunicando, ad esempio, ai clienti l'uso di un sistema chatbot IA; **2.** proteggere la privacy dei clienti e garantire che l'IA non applichi comportamenti discriminatori favorendo alcuni clienti piuttosto che altri.

5.2 RESPONSABILITA' E DIRITTI UMANI

È fondamentale che l'IA sia utilizzata in modo da rispettare i diritti umani e promuovere il benessere sociale, favorendo l'integrazione sociale, finanziaria, lavorativa.

Infatti, l'utilizzo dell'IA può certamente garantire un miglioramento dell'ambiente lavorativo migliorando l'efficienza e l'efficacia del lavoro e svolgendo le attività più operative analizzando per esempio in brevi periodi grandi quantità di dati.

Un uso diligente e responsabile di sistemi IA assicura che i medesimi possano perpetuare o ampliare pregiudizi esistenti favorendo comportamenti discriminatori ed essere utilizzata per intensificare alcune dinamiche di controllo e di violazione della privacy di dipendenti e collaboratori.

5.3 RUOLO DELL' INTELLIGENZA ARTIFICIALE

L'uso di un sistema IA deve essere rappresentare un supporto all'Amministratore Unico e qualora venga autorizzato ai lavoratori in modo da semplificarne le attività,

senza però arrivare alla sostituzione di questi ultimi in modo da non violarne i diritti. Infatti, l'IA deve essere sviluppata in modo antropocentrico garantendo che quest'ultima favorisca il benessere umano.

L'IA deve operare sempre sotto controllo umano, verificando che sia sempre un essere umano a supervisionare o a controllare le decisioni prese da modelli di IA, garantendo e verificando la qualità e l'affidabilità degli output di risposta forniti dall'IA.

È importante formare i lavoratori permettendo loro una collaborazione più proficua con l'IA e garantendo che questi abbiano le competenze per lavorare in un conteso di questo tipo.

5.4 GESTIONE DEL RISCHIO

Un sistema di gestione del rischio interattivo e continuo è essenziale per identificare, valutare e mitigare i rischi per la salute, la sicurezza e i diritti fondamentali dei lavoratori derivanti dall'uso dell'IA.

Il sistema di gestione dei rischi è inteso come un processo interattivo continuo, pianificato ed eseguito nel corso dell'intero ciclo di vita di un sistema di IA, che richiede riesami e aggiornamenti costanti e sistematici.

Tale processo si articola nelle seguenti fasi:

1) identificazione e analisi dei rischi noti e ragionevolmente prevedibili che il sistema di IA potrebbe causare alla salute, alla sicurezza e ai diritti fondamentali dei lavoratori;

2) stima e valutazione dei rischi che possono emergere quando il sistema di IA è usato conformemente alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibili;

3) valutazione di altri eventuali rischi derivanti dall'analisi dei dati raccolti;

4) adozione di misure di gestione dei rischi opportune e mirate intese ad affrontare i rischi legati all'utilizzo dell'IA.

6. GOVERNANCE DELL'INTELLIGENZA ARTIFICIALE

La governance dell'IA si riferisce ai processi, agli standard e alle misure di sicurezza che contribuiscono a garantire che i sistemi e gli strumenti di IA siano sicuri ed etici. I framework di governance dell'IA orientano la ricerca, lo sviluppo e le applicazioni di IA per garantire sicurezza, equità e rispetto dei diritti umani.

Una governance efficace dell'IA include meccanismi di supervisione che trattano rischi quali distorsioni, violazioni della privacy e uso improprio, promuovendo al contempo l'innovazione e aumentando la fiducia. Un approccio etico alla governance dell'IA richiede quindi il coinvolgimento di un'ampia gamma di stakeholder, tra cui sviluppatori di IA, utenti, funzioni di direzione e di controllo, in modo da garantire che i sistemi legati all'IA siano sviluppati e utilizzati in linea con i valori dell'impresa.

I presidi di governance che l'impresa dovrà mettere in atto mirano quindi a definire la matrice di supervisione necessaria per allineare i comportamenti dei sistemi di IA in uso all'azienda agli standard etici sopra descritti.

7. SICUREZZA E CYBERSECURITY

7.1 PROTEZIONE DEI DATI

GETOPEN attribuisce primaria importanza alla protezione dei dati personali, delle informazioni riservate e del patrimonio informativo aziendale.

L'utilizzo di applicazioni di Intelligenza Artificiale può comportare rischi di divulgazione, conservazione o trattamento non autorizzato di dati; pertanto, è fatto divieto di inserire, caricare, condividere o trattare tramite strumenti di Intelligenza Artificiale dati personali, dati aziendali, informazioni riservate o confidenziali, salvo nei casi espressamente autorizzati e nel rispetto della normativa vigente.

Ogni utilizzo autorizzato di applicazioni di Intelligenza Artificiale deve avvenire nel rispetto dei principi di liceità, correttezza, trasparenza, minimizzazione dei dati e sicurezza, nonché delle misure tecniche e organizzative adottate dalla Società ai

sensi del Regolamento (UE) 2016/679 (GDPR) e della normativa applicabile in materia di Intelligenza Artificiale.

La violazione delle presenti disposizioni in materia di protezione dei dati costituisce grave inosservanza della Policy e potrà comportare l'adozione delle misure disciplinari e contrattuali previste, oltre a eventuali responsabilità civili e amministrative.

Dunque, i dispositivi di IA devono essere conformi ai seguenti principi:

i) trasparenza e informazione: gli interessati devono essere informati in modo chiaro e comprensibile sul trattamento dei loro dati da parte di sistemi IA, inclusi eventuali

processi decisionali automatizzati;

ii) consenso e liceità: il trattamento dei dati personali da parte di sistemi di Intelligenza Artificiale deve basarsi su una base giuridica valida ai sensi dell'art. 6 del Regolamento (UE) 2016/679, individuata caso per caso in funzione delle finalità del trattamento e del contesto di utilizzo;

iii) diritti degli interessati: gli interessati hanno il diritto di accedere ai dati, rettificarli, cancellarli, opporsi al trattamento e non essere soggetti a decisioni automatizzate senza intervento umano;

iv) valutazione d'impatto: per i trattamenti IA che presentano rischi elevati, è obbligatoria una valutazione d'impatto sulla protezione dei dati.

Il GDPR pone inoltre particolare attenzione sul trattamento automatizzato dei dati personali. L'Art. 22 del GDPR (Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione) ribadisce, come principio generale, che l'interessato ha il diritto di non essere sottoposto a una decisione basata esclusivamente sul trattamento automatizzato dei propri dati, a cominciare dalla profilazione, che produca effetti giuridici che lo riguardano o che incida allo stesso modo sulla sua persona in modo significativo.

Ciò che viene infatti richiesto a chi utilizza Sistemi di IA per acquisire ed elaborare dati personali è:

a) definire le finalità del trattamento;

b) informare sull'utilizzo che si fa della tecnologia IA;

c) acquisire il consenso dell'interessato ove richiesto dalla normativa applicabile, in particolare nei casi di trattamento automatizzato o di profilazione non fondati su altra idonea base giuridica;

d) determinare la base giuridica;

e) valutare l'impatto che l'uso dell'IA esercita sugli individui (DPIA);

f) dare prospetto compiuto e completo del funzionamento della tecnologia, per individuarne i criteri di ragionamento;

g) intervenire nel caso in cui si presentino possibili occasioni di violazione dei diritti degli interessati;

h) comunicare e informare in caso di data breach;

i) implementare sistemi di logging e tracciabilità per i sistemi di IA ad alto rischio;

j) adottare misure di sicurezza rafforzate contro attacchi adversarial e tentativi di manipolazione.

7.2 MISURE DI SICUREZZA E CONTROLLO NELL'UTILIZZO DELL'INTELLIGENZA ARTIFICIALE

GETOPEN adotta adeguate misure tecniche e organizzative volte a garantire la sicurezza, l'integrità, la riservatezza e la disponibilità dei dati e delle informazioni trattate in relazione all'utilizzo di applicazioni di Intelligenza Artificiale.

In particolare, l'utilizzo autorizzato di strumenti di Intelligenza Artificiale è soggetto alle seguenti misure di sicurezza:

1. utilizzo esclusivo di strumenti e piattaforme preventivamente approvati dall'Amministratore Unico;

2. accesso consentito unicamente tramite account aziendali autorizzati, con credenziali personali e non cedibili;

3. adozione di misure di autenticazione e controllo degli accessi adeguate al livello di rischio;

4. divieto di utilizzo di applicazioni di Intelligenza Artificiale su dispositivi o reti non sicure o non autorizzate dalla Società;

5. limitazione dell'inserimento dei dati al minimo necessario per la finalità autorizzata;

6. conservazione della documentazione relativa agli utilizzi autorizzati, ove applicabile.

La Società si riserva la facoltà di effettuare attività di monitoraggio e verifica, nel rispetto della normativa vigente in materia di protezione dei dati personali, delle garanzie previste dallo Statuto dei Lavoratori, nonché delle policy aziendali in materia di utilizzo degli strumenti informatici e dei sistemi di controllo.

Eventuali incidenti di sicurezza, violazioni dei dati personali o utilizzi non conformi delle applicazioni di Intelligenza Artificiale devono essere tempestivamente segnalati all'Amministratore Unico e ai soggetti incaricati, al fine di consentire l'adozione delle misure correttive e di contenimento necessarie.

8 REVISIONE E AGGIORNAMENTO

La presente Policy è soggetta a revisione ogniqualvolta si verifichino:

- cambiamenti normativi significativi (es. piena applicazione dell'AI Act);
- introduzione di nuovi sistemi IA con profilo di rischio medio o elevato;
- modifiche sostanziali al Sistema AIMS o ai processi aziendali.

Ogni revisione dovrà essere approvata con determina dall'Amministratore Unico.

In ultimo, si precisa che anche ogni eventuale estensione dell'utilizzo di strumenti di Intelligenza Artificiale a favore di dipendenti o collaboratori potrà avvenire unicamente previa revisione formale della presente Policy, autorizzazione espressa dell'Amministratore Unico e svolgimento delle necessarie valutazioni di conformità normativa, incluse quelle in materia di protezione dei dati personali e di gestione del rischio.