

DICHIARAZIONE AZIENDALE SULL'UTILIZZO RESPONSABILE DELL'INTELLIGENZA ARTIFICIALE

Misure organizzative adottate in coerenza con il Regolamento (UE) 2024/1689 – AI Act

POSIZIONE DI PRAGMATIKA

Pragmatika utilizza strumenti di intelligenza artificiale esclusivamente come supporto alle attività professionali. Gli output non sostituiscono il giudizio, la responsabilità editoriale o le decisioni delle persone. Alla data del presente documento, gli impieghi autorizzati sono riconducibili a funzioni di supporto a rischio minimo o limitato; non sono autorizzati usi vietati né sistemi destinati a decisioni ad alto rischio.

1. Scopo e principi generali

Il presente documento definisce le regole interne adottate da Pragmatika S.r.l. per l'utilizzo di sistemi di intelligenza artificiale generativa e per la gestione dei relativi rischi. Le misure sono basate sui principi di proporzionalità, trasparenza, protezione dei dati, supervisione umana, sicurezza, rispetto della proprietà intellettuale e responsabilità professionale.

La classificazione prevista dall'AI Act dipende soprattutto dalla finalità e dal contesto d'uso, non soltanto dal nome dello strumento. Ogni nuova applicazione, integrazione o modifica significativa deve quindi essere valutata prima dell'attivazione.

2. Strumenti autorizzati e ambiti di utilizzo

Strumento	Utenti autorizzati	Finalità ammesse	Controlli principali
ChatGPT	Personale dipendente, tramite account aziendale	Bozze, sintesi, brainstorming, supporto redazionale e analisi preliminari	Opzione di utilizzo dei contenuti per il miglioramento dei modelli disattivata; cancellazione delle conversazioni a fine attività; controllo umano
Claude	Solo personale espressamente autorizzato	Sviluppo di software per uso interno e analisi di mercato	Revisione del codice, test, esclusione di credenziali e dati riservati, verifica delle fonti e delle conclusioni
Higgsfield	Solo personale espressamente autorizzato	Generazione e rielaborazione di immagini	Verifica diritti, trasparenza quando necessaria, divieto di contenuti ingannevoli o uso non autorizzato dell'immagine di persone reali

Regola di accesso: il personale dipendente può utilizzare esclusivamente ChatGPT tramite l'account aziendale. Claude e Higgsfield sono riservati ai soggetti incaricati dalla Direzione. È vietato utilizzare account personali o strumenti gratuiti/non approvati per attività aziendali.

3. Regole operative obbligatorie

3.1 Protezione dei dati e riservatezza

- Applicazione del principio di minimizzazione: nei prompt devono essere inserite solo le informazioni strettamente necessarie allo svolgimento dell'attività.
- Divieto di inserire password, chiavi API, credenziali, database completi, documenti riservati dei clienti, dati finanziari non pubblici o segreti commerciali.
- I dati personali devono essere anonimizzati o pseudonimizzati. Le categorie particolari di dati personali non devono essere inserite, salvo preventiva autorizzazione, specifica base giuridica e adeguate misure di protezione.
- Il contenuto utile prodotto dall'IA deve essere trasferito negli archivi aziendali autorizzati; la chat non deve essere utilizzata come archivio documentale.

3.2 Impostazioni, conservazione e cancellazione delle chat

- Per ChatGPT è disattivata l'opzione che consente l'utilizzo delle conversazioni per l'addestramento o il miglioramento dei modelli, secondo le impostazioni disponibili nel servizio.
- Al termine del lavoro, il dipendente deve cancellare la conversazione e gli eventuali file caricati, compatibilmente con le funzionalità e i tempi tecnici della piattaforma.
- Non devono essere creati link pubblici alle conversazioni né condivise chat aziendali con soggetti non autorizzati.

3.3 Supervisione umana e responsabilità

- Ogni output è considerato una bozza e deve essere verificato da una persona competente prima dell'utilizzo interno o della pubblicazione.
- La verifica comprende accuratezza dei fatti, aggiornamento delle fonti, coerenza, possibili bias, rischi reputazionali, correttezza linguistica e tutela della riservatezza.
- L'IA non può assumere decisioni autonome che producano effetti giuridici, economici, professionali o reputazionali su clienti, dipendenti, candidati o altri soggetti.
- La responsabilità finale del contenuto, del software, dell'analisi o dell'immagine resta in capo al professionista e alla Direzione di Pragmatika.

3.4 Trasparenza e contenuti generati artificialmente

- Qualora Pragmatika attivi in futuro chatbot o assistenti rivolti al pubblico, l'utente sarà informato in modo chiaro che sta interagendo con un sistema di IA, salvo che ciò risulti già evidente dal contesto.
- Immagini, audio, video o altri contenuti artificiali/manipolati sono segnalati quando possono essere scambiati per reali, quando rappresentano persone o fatti reali, oppure quando la segnalazione è richiesta dall'articolo 50 dell'AI Act.
- I testi destinati alla pubblicazione sono sempre sottoposti a revisione editoriale umana; Pragmatika ne assume la responsabilità e non pubblica automaticamente contenuti generati dall'IA.

3.5 Copyright, marchi e diritti delle persone

- È vietato richiedere la riproduzione sostanziale di opere protette, materiali proprietari, loghi o asset di terzi senza autorizzazione o licenza.
- Prima dell'uso esterno vengono verificati fonti, citazioni, licenze, marchi, diritti d'immagine e condizioni contrattuali del fornitore dello strumento.
- Non è consentita la creazione di rappresentazioni ingannevoli di persone reali, né l'uso della loro immagine o voce senza adeguato titolo e consenso quando necessario.

4. Controlli specifici per strumento

4.1 ChatGPT – attività ordinarie del personale

- Utilizzo esclusivo tramite l'account aziendale autorizzato; sono vietati account personali, plug-in non approvati e collegamenti a fonti aziendali senza autorizzazione.
- Impiego consentito per ideazione, organizzazione, sintesi, riscrittura, traduzione, preparazione di bozze e analisi preliminari. Il risultato deve essere rielaborato e validato dal professionista.
- Le conversazioni devono essere cancellate dopo la conclusione dell'attività e non possono contenere informazioni confidenziali non minimizzate.

4.2 Claude – sviluppo software interno

- Il codice generato è sempre sottoposto a code review umana, test funzionali e di sicurezza prima dell'utilizzo.
- Sono esclusi dai prompt password, token, chiavi private, configurazioni di produzione, dati reali dei clienti e informazioni che possano compromettere la sicurezza dei sistemi.
- Le librerie e le dipendenze suggerite devono essere verificate per provenienza, licenza, aggiornamento e vulnerabilità note.
- Non è consentito il rilascio automatico in produzione. Ogni distribuzione richiede approvazione umana, tracciabilità delle modifiche e possibilità di rollback.
- Qualora il software incorpori funzioni di IA destinate a incidere su persone o decisioni, l'uso deve essere sospeso fino a una nuova valutazione di rischio, privacy e conformità.

4.3 Claude – analisi di mercato

- Le informazioni devono essere confrontate con fonti attendibili, aggiornate e identificabili; fatti, stime e inferenze devono essere distinti chiaramente.
- Le conclusioni generate dall'IA non vengono utilizzate come unico fondamento di decisioni commerciali o strategiche.
- Dati personali, liste di contatti o informazioni non pubbliche sui concorrenti non devono essere trattati senza una base legittima e una specifica autorizzazione.

4.4 Higgsfield – generazione di immagini

- Ogni immagine è verificata da un professionista prima dell'impiego, con attenzione a contenuti falsi, discriminatori, lesivi o suscettibili di indurre in errore.
- È vietato generare categorizzazioni biometriche, riconoscimenti facciali, rappresentazioni discriminatorie o immagini che deducano caratteristiche sensibili delle persone.
- L'uso di volti, corpi, voce, marchi, prodotti o ambienti riconoscibili richiede la verifica dei relativi diritti. La natura artificiale del contenuto viene indicata quando necessario per evitare inganno o in applicazione delle norme vigenti.

5. Usi vietati dalla policy aziendale

- Manipolazione subliminale o ingannevole delle persone, sfruttamento di vulnerabilità, social scoring o pratiche suscettibili di causare danni.
- Identificazione biometrica, creazione di database facciali, categorizzazione biometrica per dedurre dati sensibili o riconoscimento delle emozioni sul luogo di lavoro.
- Selezione, valutazione, classificazione, promozione o cessazione del personale mediante decisioni automatizzate.
- Decisioni in materia sanitaria, legale, creditizia, assicurativa, accesso a servizi essenziali, istruzione, sicurezza o altre aree ad alto rischio.
- Pubblicazione automatica di testi, immagini o software senza controllo umano; impersonificazione, deepfake ingannevoli, disinformazione o produzione di contenuti illeciti.

6. Governance, formazione e controllo

Pragmatika considera l'alfabetizzazione sull'intelligenza artificiale un requisito organizzativo. Il personale autorizzato riceve indicazioni proporzionate alle mansioni, ai rischi e agli strumenti utilizzati, con particolare attenzione a limiti dei modelli, allucinazioni, protezione dei dati, sicurezza, copyright, bias e trasparenza.

6.1 Misure organizzative attive

✓	Elenco degli strumenti e degli utenti autorizzati.
✓	Regole scritte sui dati che possono o non possono essere inseriti nei prompt.
✓	Supervisione umana obbligatoria e divieto di pubblicazione automatica.
✓	Disattivazione dell'utilizzo delle conversazioni di ChatGPT per il miglioramento dei modelli, secondo le impostazioni del servizio.
✓	Cancellazione delle conversazioni al termine dell'attività.
✓	Controlli specifici per codice, analisi di mercato e immagini.
✓	Segnalazione immediata di errori, divulgazioni accidentali, contenuti lesivi o incidenti di sicurezza.
✓	Revisione della policy almeno annuale e ogni volta che cambiano strumenti, finalità, norme o linee guida applicabili.

6.2 Gestione delle anomalie

Chiunque rilevi un uso non autorizzato, un possibile data breach, un output gravemente errato o discriminatorio, una violazione del copyright o un rischio di sicurezza deve interrompere l'utilizzo e informare immediatamente la Direzione. La Direzione valuta la cancellazione dei dati, la sospensione dello strumento, le eventuali comunicazioni al cliente o alle autorità e le misure correttive.

7. Dichiarazione conclusiva

Pragmatika S.r.l. adotta un approccio prudente e proporzionato all'utilizzo dell'intelligenza artificiale. Gli strumenti generativi sono impiegati come ausilio alle competenze professionali, con accessi controllati, minimizzazione dei dati, supervisione umana, verifica delle fonti, tutela dei diritti e tracciabilità delle responsabilità.

La presente policy descrive le misure organizzative in vigore alla data indicata. Ogni nuovo caso d'uso sarà sottoposto a preventiva valutazione per stabilire il livello di rischio e gli eventuali adempimenti ulteriori previsti dall'AI Act, dal GDPR, dalla normativa sul diritto d'autore e dalle disposizioni applicabili.

Riferimenti principali

Regolamento (UE) 2024/1689, in particolare artt. 4, 5, 26, 50 e 99; Regolamento (UE) 2016/679 (GDPR); normativa nazionale ed europea in materia di protezione dei dati, diritto d'autore e sicurezza informatica. Applicazione e interpretazione sono soggette a eventuali aggiornamenti normativi e linee guida delle autorità competenti.

Per Pragmatika S.r.l.

Rossella Lucangelo – CEO

Firma Rossella Lucangelo