

AI POLICY

Regole per l'uso degli Agent di intelligenza artificiale Pangea AI HSE

1. Scopo della AI Policy

La presente AI Policy disciplina l'utilizzo degli Agent basati su intelligenza artificiale disponibili nella piattaforma **Pangea AI HSE**.

La policy definisce:

- regole di utilizzo;
 - responsabilità dell'utente;
 - limiti degli output;
 - obblighi di controllo umano;
 - regole sui dati inseriti;
 - usi vietati;
 - gestione di anomalie e incidenti;
 - principi di trasparenza verso utenti e organizzazioni clienti.
-

2. Campo di applicazione

La presente policy si applica a:

- clienti;
 - amministratori account;
 - utenti autorizzati;
 - consulenti;
 - referenti aziendali;
 - organizzazioni che acquistano o utilizzano Pangea AI HSE;
 - soggetti che utilizzano output generati o assistiti dagli Agent.
-

3. Che cosa offre la piattaforma

Pangea AI HSE mette a disposizione Agent, cioè moduli basati su sistemi di intelligenza artificiale, progettati per supportare attività professionali in ambito:

- salute e sicurezza sul lavoro;
- ambiente;
- antincendio;
- cantieri;
- formazione;
- privacy;
- compliance;
- sistemi di gestione;
- document management;
- altri ambiti HSE e organizzativi.

Gli Agent possono assistere l'utente nella raccolta dati, analisi, classificazione, predisposizione di bozze, tabelle, checklist, piani, procedure, documenti e materiali professionali.

4. Trasparenza sull'uso dell'AI

L'utente sa, prima dell'interazione, che sta utilizzando un sistema basato su intelligenza artificiale.

I contenuti prodotti dagli Agent possono essere generati, rielaborati, ordinati o sintetizzati automaticamente.

L'utente deve informare eventuali destinatari quando un contenuto è stato generato o assistito da AI, se ciò è richiesto dalla normativa, dalle procedure interne, dal contesto professionale o dalle regole di trasparenza applicabili.

5. Ruoli e responsabilità

Pangea gestisce la piattaforma, gli Agent, le configurazioni, la sicurezza del servizio e le regole generali di utilizzo.

Il cliente governa l'uso degli Agent da parte dei propri utenti autorizzati.

L'utente è responsabile:

- dei dati inseriti;
- della liceità delle informazioni caricate;
- della pertinenza dei documenti;

- della verifica degli output;
- della validazione professionale;
- dell'eventuale uso ufficiale del risultato;
- della pubblicazione o trasmissione a terzi.

La persona competente dell'organizzazione approva la versione finale del documento secondo le responsabilità interne e normative applicabili.

6. Metodo di lavoro

L'utilizzo degli Agent deve seguire un metodo di lavoro controllato:

1. definire il perimetro della richiesta;
 2. caricare solo dati pertinenti;
 3. distinguere dati certi, dati mancanti e dati da verificare;
 4. controllare fonti, allegati e informazioni aziendali;
 5. verificare riferimenti normativi, calcoli e conclusioni;
 6. correggere errori o incompletezze;
 7. validare il risultato con persona competente;
 8. utilizzare l'output solo dopo approvazione.
-

6-bis. Metodo FGA — Focused Governance Architecture

Gli Agent Pangea AI HSE che adottano FGA (Focused Governance Architecture, architettura di governo focalizzata) applicano controlli lungo l'elaborazione: definiscono il perimetro della richiesta, distinguono l'origine dei dati e delle fonti, gestiscono le autorizzazioni e verificano la coerenza dell'output. Il metodo assiste un lavoro documentale tracciabile; non certifica la correttezza del risultato e non sostituisce la revisione della persona competente prevista al punto 7.

6-bis.1 Controlli nelle tre fasi

Checkpoint A, prima dell'elaborazione: l'Agent identifica obiettivo e ambito, verifica i dati e gli allegati disponibili, segnala quelli mancanti e applica il controllo di accesso alle fonti esterne. Quando il flusso richiede una presa d'atto iniziale (ACK) o un'approvazione dell'utente, attende tale passaggio prima di proseguire.

Checkpoint B, durante l'elaborazione: l'Agent distingue i fatti forniti dal cliente tramite richiesta, conferme e allegati dalle regole, dai modelli e dai materiali metodologici usati per elaborare il contenuto. Non attribuisce al cliente dati ricavati soltanto da esempi o template; evidenzia incertezze, contraddizioni, lacune e verifiche necessarie.

Riferimenti normativi, calcoli e conclusioni devono essere controllabili rispetto alle fonti effettivamente disponibili.

Checkpoint C, prima della consegna: l'Agent esamina la coerenza tra richiesta, fonti utilizzate, passaggi compiuti e risultato; indica eventuali riserve o blocchi e separa l'output destinato all'uso professionale dalle informazioni operative di audit. L'utente verifica e approva l'output secondo i punti 7, 11 e 12 prima di adottarlo o trasmetterlo.

6-bis.2 Accesso al Web e autorizzazione

Per gli Agent soggetti al presidio FGA l'accesso al Web è disabilitato per impostazione predefinita. Prima di una ricerca online, l'Agent verifica se la ricerca sia necessaria, ne delimita l'oggetto e controlla che l'utente l'abbia autorizzata espressamente, in anticipo e per quello specifico perimetro. L'utente può scrivere, ad esempio, «AUTORIZZO RICERCA WEB PER [oggetto specifico]». Richieste generiche di “verificare”, “aggiornare” o “procedere” non costituiscono di per sé autorizzazione alla ricerca online. Se l'autorizzazione manca o non copre la ricerca proposta, l'Agent non esegue la chiamata Web e segnala il limite; la provenienza di eventuali fonti online utilizzate è distinta da documenti e informazioni del cliente.

6-bis.3 Semaforo FGA, audit e limiti

Il Semaforo FGA sintetizza l'esito complessivo dei controlli applicabili alla singola elaborazione, non soltanto del controllo Web: VERDE se i controlli risultano superati e non vi sono riserve aperte; GIALLO se restano dati, verifiche o autorizzazioni da risolvere senza che sia stata accertata una violazione; ROSSO in caso di violazione o di blocco che impedisce di proseguire regolarmente. Un tentativo di accesso Web fermato prima della ricerca non equivale a un accesso non autorizzato effettivamente eseguito. Il semaforo è ricalcolato per ogni nuova elaborazione; le informazioni delle elaborazioni precedenti restano nel relativo storico di audit, consultabile con il comando «AUDIT FGA» o «MOSTRA AUDIT FGA» ove previsto dall'Agent. Il colore VERDE non equivale a certificazione, parere professionale o approvazione del documento.

7. Controllo umano obbligatorio

Gli output degli Agent:

- non sono automaticamente documenti ufficiali;
- non sono certificazioni;
- non sono pareri legali;
- non sostituiscono valutazioni obbligatorie;
- non sostituiscono firme, approvazioni o responsabilità professionali;
- non devono essere usati senza revisione.

Prima di utilizzare un output, l'utente deve verificare:

- correttezza dei dati;
 - completezza delle informazioni;
 - coerenza con il caso concreto;
 - aggiornamento normativo;
 - adeguatezza tecnica;
 - eventuali errori o omissioni;
 - presenza di dati personali o riservati;
 - necessità di approvazione interna.
-

8. Dati in ingresso

L'utente deve inserire solo dati:

- pertinenti;
- aggiornati;
- necessari;
- leciti;
- proporzionati;
- coerenti con lo scopo professionale.

Ove possibile, i dati personali devono essere minimizzati o pseudonimizzati.

Non devono essere inseriti dati eccedenti rispetto alla finalità della lavorazione.

9. Dati particolari, giudiziari o riservati

L'utente deve evitare di caricare:

- dati sanitari;
- dati giudiziari;
- dati biometrici;
- dati sindacali;
- dati relativi a opinioni politiche;
- dati relativi a convinzioni religiose o filosofiche;
- password;
- chiavi di accesso;
- segreti industriali non necessari;
- informazioni riservate non pertinenti.

L'inserimento di tali dati è ammesso solo se necessario, lecito, autorizzato e protetto da misure adeguate.

10. Usi vietati

È vietato utilizzare gli Agent per:

- attività illecite;
- inganno;
- frode;
- discriminazione;
- diffamazione;
- elusione di obblighi di legge;
- generazione di contenuti falsi o manipolativi;
- decisioni significative su persone senza valutazione giuridica e presidio umano;
- sorveglianza non autorizzata;
- profilazione illecita;
- trattamento di dati personali senza base giuridica;

- pubblicazione di output non verificati;
 - trasferimento automatico di output in documenti ufficiali senza revisione;
 - rimozione di avvisi, disclaimer, marcatori o limitazioni d'uso.
-

11. Limiti degli output

Gli Agent possono generare:

- errori;
- riferimenti incompleti;
- contenuti non aggiornati;
- interpretazioni non applicabili;
- sintesi eccessive;
- omissioni;
- formulazioni non idonee al caso concreto.

Per questo motivo ogni output deve essere verificato prima dell'uso.

Un testo generato non equivale, da solo, a:

- valutazione dei rischi;
 - documento privacy adottato;
 - parere legale;
 - certificazione;
 - atto firmato;
 - documento ufficiale;
 - validazione tecnica;
 - adempimento completato.
-

12. Pubblicazione e comunicazione a terzi

Prima di pubblicare o trasmettere a terzi un output generato o assistito da AI, l'utente deve:

- verificarne accuratezza e completezza;
 - rimuovere dati personali non necessari;
 - controllare eventuali informazioni riservate;
 - validare il contenuto con soggetto competente;
 - indicare l'uso di AI quando richiesto;
 - rispettare le regole interne e contrattuali;
 - verificare la compatibilità con privacy, copyright, segreti commerciali e obblighi professionali.
-

13. Competenze e formazione

Il cliente deve assicurare che gli utenti autorizzati dispongano di istruzioni e competenze adeguate per utilizzare gli Agent.

Gli utenti devono conoscere:

- limiti dell'AI;
 - rischi di errore;
 - necessità di verifica;
 - regole privacy;
 - divieti di caricamento dati;
 - procedure interne;
 - obblighi di riservatezza;
 - modalità di segnalazione anomalie.
-

14. Sicurezza

Pangea gestisce versioni, funzionalità, sicurezza del servizio e canali di segnalazione.

L'utente deve:

- custodire le credenziali;
 - non condividere account;
 - non aggirare controlli o limiti tecnici;
 - non scaricare o esportare dati senza autorizzazione;
 - non usare la piattaforma da dispositivi o reti non sicuri;
 - segnalare accessi anomali o sospetti.
-

15. Segnalazioni e incidenti

Se l'utente rileva:

- output potenzialmente dannoso;
- anomalia tecnica;
- errore grave;
- accesso non autorizzato;
- divulgazione accidentale di dati;
- perdita di riservatezza;
- sospetto data breach;
- uso improprio dell'account;

deve interrompere l'uso del risultato coinvolto, conservare le evidenze utili e scrivere a:

privacy@pangeaconsulenze.com

Pangea valuta la segnalazione e applica le proprie procedure di gestione incidenti secondo legge e accordi con il cliente.

16. Aggiornamento della AI Policy

La presente policy è aggiornata al **28 settembre 2026**.

Pangea può aggiornarla in caso di:

- modifica degli Agent;
 - nuove funzionalità;
 - modifica normativa;
 - modifica dei fornitori tecnologici;
 - modifiche di sicurezza;
 - incidenti;
 - audit;
 - evoluzione del servizio.
-