

[illegible]

Indice

1. Introduzione	3
1.1 Scopo del documento	3
1.2 Ambito di applicazione	3
1.3 Riesame periodico del documento.....	3
2. Visione e obiettivi della politica.....	5
2.1 Visione di PA Advice sull'Intelligenza Artificiale.....	5
2.2 Obiettivi della politica	5
3. Governance dell'Intelligenza Artificiale.....	8
3.1 Ruoli e responsabilità	8
3.2 Modello organizzativo	8
3.3 Coordinamento con le altre politiche aziendali	9
4. Approccio basato sul rischio.....	10
4.1 Classificazione del rischio	10
4.2 Valutazione e trattamento del rischio	10
4.3 Pratiche vietate	10
4.4 Valutazione degli impatti dei sistemi di IA.....	11
5. Impegni di PA Advice	12
5.1 Impegni verso il personale	12
5.2 Impegni verso i clienti	12
5.3 Impegni verso i fornitori.....	12
5.4 Impegni verso gli stakeholder e la collettività	13
6. Tutela dei dati, riservatezza e proprietà intellettuale	14
7. Sistema di gestione, monitoraggio e miglioramento continuo del SGIA	15
7.1 Documentazione del sistema di gestione.....	15
7.2 Audit e riesame della direzione.....	15
7.3 Obiettivi del Sistema di Gestione IA	15
7.4 Comunicazione.....	16

7.5	Segnalazioni.....	16
8.	Violazioni e misure.....	17

1. Introduzione

1.1 Scopo del documento

Il presente documento stabilisce la Politica per la Gestione dell'Intelligenza Artificiale (di seguito "AI Policy") di PA Advice S.p.A., espressione formale degli orientamenti e degli indirizzi dell'alta direzione in materia di sviluppo, fornitura, integrazione e utilizzo dei sistemi di IA (§3.5 *politica*; §5.2).

La Policy costituisce il documento di vertice del Sistema di Gestione dell'Intelligenza Artificiale di PA Advice ed è declinata operativamente da procedure, linee guida, registri e modelli, che ne assicurano l'applicazione concreta e la verificabilità; la Policy è, inoltre, coerente e integrata con le altre politiche aziendali di PA Advice, in particolare con quelle relative alla qualità, alla sicurezza delle informazioni, alla protezione dei dati personali, alla compliance e all'etica professionale.

Il documento è classificato come PAA PUBLIC, secondo i livelli di classificazione delle informazioni previsti dall'azienda, in quanto accessibile a tutto il personale interno all'organizzazione.

1.2 Ambito di applicazione

La presente Policy deve essere seguita da tutto il personale di PA Advice nonché ai collaboratori, consulenti e professionisti esterni, fornitori e i partner che sviluppano, forniscono o utilizzano sistemi di IA per conto di PA Advice o che intervengono in progetti in cui tali sistemi sono utilizzati. I destinatari sono tenuti a conoscere, rispettare e far rispettare la Policy nell'ambito delle proprie attività e responsabilità.

La Policy si applica a tutte le attività di PA Advice che riguardano l'IA: la progettazione, lo sviluppo, l'implementazione e il monitoraggio dei sistemi di IA forniti alla Pubblica Amministrazione, inclusi quelli che integrano modelli di terzi (SLM/LLM), nonché l'utilizzo di strumenti di IA a supporto dei processi interni dell'organizzazione.

1.3 Riesame periodico del documento

La Policy è sottoposta a verifica annuale nell'ambito del riesame della direzione e a revisione triennale, nonché ogni qual volta intervengano modifiche significative del quadro normativo, dell'organizzazione aziendale, dei sistemi di IA utilizzati o delle risultanze del monitoraggio.

Le revisioni sostanziali sono approvate dal Consiglio di Amministrazione; gli aggiornamenti non sostanziali possono essere disposti dall'AI Officer, dandone informativa al Comitato IA. Il versionamento è tracciato nella tabella in copertina.

2. Visione e obiettivi della politica

2.1 Visione di PA Advice sull'Intelligenza Artificiale

PA Advice considera l'Intelligenza Artificiale una leva strategica di trasformazione della Pubblica Amministrazione, in grado di migliorare la qualità dei servizi al cittadino, l'efficienza dei processi amministrativi e la capacità decisionale degli enti. Tale potenziale, tuttavia, può essere pienamente realizzato solo a condizione che l'IA sia progettata, sviluppata e utilizzata in modo affidabile, trasparente e centrato sulla persona, nel pieno rispetto dei diritti fondamentali, dei valori costituzionali e del quadro normativo vigente.

Coerentemente con la propria storia ultraventennale al servizio della PA italiana, PA Advice si impegna a essere per i propri clienti un partner di riferimento per l'adozione consapevole dell'IA, contribuendo alla diffusione di pratiche conformi e di alta qualità nell'ecosistema della Pubblica Amministrazione. L'adozione dell'IA all'interno dell'organizzazione, difatti, si integra con i principi di etica, risk management, trasparenza e responsabilità.

2.2 Obiettivi della politica

PA Advice fonda l'adozione e l'utilizzo dei sistemi di IA sui seguenti principi, che orientano ogni scelta strategica, organizzativa e operativa.

- **Legalità e conformità.** PA Advice sviluppa, integra e utilizza i sistemi e gli strumenti di IA nel rispetto dei requisiti legali e regolamentari applicabili, in particolare il Regolamento (UE) 2024/1689 (AI Act), il GDPR e le indicazioni applicabili per l'adozione dell'IA nella Pubblica Amministrazione. L'organizzazione individua e si astiene dalle pratiche di IA vietate e tratta con specifica attenzione i sistemi ad alto rischio.
- **Supervisione umana (human oversight).** Tutti i sistemi e gli strumenti di IA, sia rivolti alla Pubblica Amministrazione sia di uso interno, che incidono su persone fisiche o supportano decisioni rilevanti sono impiegati garantendo un'adeguata supervisione umana, proporzionata all'impatto:
 - nel processo di sviluppo del software sono previsti gate di approvazione umana lungo le fasi del ciclo di vita, per cui nessuna fase rilevante avanza senza la validazione e l'autorizzazione esplicita delle figure competenti;
 - nell'utilizzo di strumenti di IA a supporto delle attività interne, come la produzione di documentazione, l'IA assiste il personale ma non lo

sostituisce, e l'output è sempre verificato e approvato dalla persona responsabile prima di essere considerato valido, utilizzato o consegnato, così che la responsabilità del prodotto finale resta in capo al personale.

Il livello di supervisione umana è definito in funzione del livello di rischio del sistema di IA e include, ove necessario, la possibilità di intervento, validazione e revisione delle decisioni supportate o generate dal sistema.

- **Correttezza e non discriminazione (fairness).** PA Advice progetta, sviluppa e utilizza i sistemi e gli strumenti di IA con l'obiettivo di prevenire bias e discriminazioni indesiderate verso persone o gruppi, prestando particolare attenzione ai contesti della Pubblica Amministrazione in cui gli esiti possono incidere su diritti, prestazioni o opportunità delle persone; a tal fine adotta misure lungo l'intero ciclo di vita — dalla selezione e preparazione dei dati alla verifica e validazione del modello — per individuare, valutare e mitigare gli effetti distorsivi, anche quando derivano da modelli di terzi integrati nei propri sistemi. I requisiti e i controlli sulla qualità dei dati che supportano questo principio sono definiti nelle relative procedure operative (vedi **PO-AI-03**).
- **Trasparenza e spiegabilità (transparency and explainability).** PA Advice assicura che le parti interessate dispongano delle informazioni necessarie a comprendere il funzionamento, gli scopi e i limiti dei sistemi di IA, in misura proporzionata al contesto e all'impatto; in particolare, gli utilizzatori sono informati quando interagiscono con un sistema di IA o ne ricevono gli output, e l'organizzazione documenta i fattori rilevanti che influenzano i risultati del sistema in modo comprensibile agli esseri umani.
- **Sicurezza e protezione dei dati.** PA Advice si impegna a sviluppare e utilizzare i sistemi e gli strumenti di IA preservando la riservatezza, l'integrità e la disponibilità delle informazioni trattate e tutelando i dati personali in ogni fase del ciclo di vita. La sicurezza è considerata fin dalla progettazione e lungo l'esercizio dei sistemi, gestendo le minacce specifiche dell'IA — ad esempio data poisoning, model stealing, model inversion — oltre ai rischi tradizionali, e prestando particolare attenzione ai dati immessi nei modelli di terzi integrati o utilizzati internamente. Questo impegno vale sia per i sistemi forniti alla Pubblica Amministrazione sia per gli strumenti di IA di uso interno.
- **Safety e robustezza.** PA Advice progetta e impiega i sistemi di IA affinché operino in modo affidabile e prevedibile nelle condizioni d'uso definite, senza comportare pericoli per le persone, e affinché mantengano prestazioni adeguate anche a fronte di dati o condizioni diversi da quelli attesi; a tal fine prevede misure di verifica e validazione, criteri di accettazione delle prestazioni e gestione dei guasti prevedibili lungo il ciclo di vita, con specifica attenzione

ai fenomeni di degrado nel tempo (concept drift, data drift). Sul fronte dell'utilizzo, PA Advice presta attenzione alla selezione dei sistemi e dei modelli di terzi che integra o impiega, valutandone affidabilità, robustezza e idoneità all'uso previsto prima della loro adozione e monitorandone il comportamento nel tempo. I criteri e le misure operative sono definiti nella procedura di ciclo di vita (vedi **PO-AI-03**); i criteri di selezione e qualifica dei fornitori e dei modelli di terzi sono disciplinati nella procedura dedicata (vedi **PO-AI-06**).

- **Accountability.** PA Advice mantiene una chiara attribuzione di responsabilità per i sistemi e gli strumenti di IA lungo l'intero ciclo di vita, individuando chi risponde delle diverse fasi e decisioni e assicurando di poter rendere conto del proprio operato alle parti interessate e, ove previsto, alle autorità di vigilanza. Quando nel ciclo di vita intervengono fornitori, partner o clienti, le responsabilità sono ripartite e documentate in modo appropriato. I ruoli e le responsabilità sono definiti nell'organigramma e nella matrice dei ruoli del SGIA (vedi **SIST-AI-05**); la ripartizione delle responsabilità con le terze parti è disciplinata nella procedura dedicata (vedi **PO-AI-06**).
- **Uso responsabile dei modelli e dei sistemi di terzi.** PA Advice utilizza i modelli e i sistemi di IA di terzi (SLM/LLM) – sia quando li integra nei propri prodotti per la Pubblica Amministrazione, sia quando li impiega a supporto dei processi interni – in modo conforme allo scopo previsto, alle condizioni d'uso e alla documentazione fornita dal fornitore, e coerentemente con i principi della presente Policy. Prima dell'adozione l'organizzazione valuta l'idoneità della soluzione di terzi rispetto ai propri obiettivi e ne verifica nel tempo l'allineamento; eventuali utilizzi non previsti sono oggetto di valutazione specifica.
- **Qualità dei dati.** PA Advice definisce e applica requisiti di qualità per i dati utilizzati nello sviluppo e nell'esercizio dei sistemi di IA, assicurando che siano adeguati, rappresentativi e idonei allo scopo previsto, e governando la loro provenienza e preparazione lungo il ciclo di vita. La qualità dei dati è presidiata anche in funzione dei suoi effetti su correttezza e prestazioni dei sistemi. I requisiti e i processi operativi sulla qualità e gestione dei dati sono definiti nella procedura dedicata (vedi **PO-AI-03** e la procedura di qualità dei dati).
- **Sostenibilità e impatto ambientale.** PA Advice considera gli impatti ambientali connessi allo sviluppo e all'utilizzo dei sistemi di IA, in particolare quelli derivanti dal consumo di risorse computazionali, e tiene conto di tali impatti nelle proprie scelte tecnologiche, nel quadro degli obiettivi generali di sostenibilità dell'organizzazione. La rilevanza del tema, anche in relazione al cambiamento climatico, è valutata nell'analisi del contesto (vedi **SIST-AI-01**).

3. Governance dell'Intelligenza Artificiale

3.1 Ruoli e responsabilità

PA Advice adotta un modello di governance dell'IA che integra le funzioni di indirizzo strategico, gestione operativa e controllo.

I principali ruoli, le cui specifiche attribuzioni sono definite e specificati nell'organigramma IA (SIST-AI-05), sono:

- **Consiglio di Amministrazione** — approva la presente Policy, ne autorizza le revisioni sostanziali e definisce gli indirizzi strategici in materia di IA.
- **Direzione** — [assicura l'attuazione degli indirizzi strategici definiti dal Consiglio di Amministrazione in materia di IA; conduce il Riesame della Direzione SGIA e approva lo scope del SGIA.](#)
- **AI Officer/ Responsabile della Sicurezza delle Informazioni** — è la figura aziendale di riferimento per la corretta applicazione della Policy e per il coordinamento del Sistema di Gestione dell'IA, anche in relazione al percorso di certificazione ISO/IEC 42001; l'AI Officer mantiene e aggiorna il registro dei sistemi di IA autorizzati per l'utilizzo interno, ivi inclusi gli strumenti di terzi impiegati dal personale nello svolgimento delle proprie attività, e definisce le condizioni di utilizzo accettabile; sovrintende agli aspetti di sicurezza informatica connessi all'utilizzo e alla fornitura di sistemi di IA.
- **Comitato IA** — organo collegiale con funzioni consultive e di indirizzo operativo, composto dai rappresentanti delle principali funzioni aziendali (direzione, CdC, BU consulenza, tecnologia, compliance, sicurezza, risorse umane).
- **Data Protection Officer (DPO)** — [assicura la coerenza dell'utilizzo dell'IA con la normativa sulla protezione dei dati personali e contribuisce alle valutazioni d'impatto.](#)
- **Responsabili di progetto** — assicurano l'applicazione della Policy nei progetti che gestiscono, in particolare nei rapporti con i clienti.
- **Personale e collaboratori** — utilizzano i sistemi di IA nel rispetto della Policy, delle procedure operative e delle istruzioni ricevute.

3.2 Modello organizzativo

Le linee di riporto, i flussi di autorizzazione e di escalation, nonché le interazioni tra i ruoli sopra indicati, sono definiti nel documento SIST-AI-05 e nelle procedure di Livello 2 collegate alla presente Policy. [I suddetti documenti, congiuntamente alla presente Policy, sono pubblicati nel canale interno aziendale così da essere accessibili a tutti gli interessati.](#)

3.3 Coordinamento con le altre politiche aziendali

La presente Policy si coordina con le altre politiche e i regolamenti aziendali di PA Advice che disciplinano ambiti intersecanti con l'utilizzo e la fornitura di sistemi di IA. In particolare:

- **Linee d'uso degli strumenti AI** — cosa si può fare, cosa richiede cautela e cosa è vietato.
- **Regolamento in materia di protezione dei dati personali** (GDPR-002)— il trattamento di dati personali nei sistemi di IA avviene in coerenza con il presente documento e in coordinamento con il DPO;
- **Regolamento di utilizzo degli strumenti informatici** (REG001)— il regolamento è aggiornato per includere le regole di utilizzo degli strumenti AI autorizzati e i divieti specifici, con rimando alla presente Policy e alle Linee guida per l'uso dell'IA per il personale (LG-AI-01);
- **Codice etico IA** — i principi e i valori etici adottati da PA Advice si applicano anche allo sviluppo, alla fornitura e all'utilizzo dei sistemi di IA, che devono svolgersi in coerenza con essi.

4. Approccio basato sul rischio

4.1 Classificazione del rischio

PA Advice adotta un approccio basato sul rischio, coerente con la classificazione dell'AI Act, che distingue tra pratiche vietate, sistemi ad alto rischio, sistemi a rischio limitato e sistemi a rischio minimo. La classificazione è applicata sia ai sistemi utilizzati internamente sia a quelli oggetto di servizi resi ai clienti.

La valutazione del rischio integra la classificazione dell'AI Act con i criteri previsti dalla norma ISO/IEC 23894, tenendo conto della probabilità di accadimento, della gravità degli impatti e del contesto specifico di utilizzo del sistema di IA.

4.2 Valutazione e trattamento del rischio

Per ogni sistema di IA rientrante nell'ambito della Policy è prevista una valutazione del rischio, condotta secondo le procedure operative dedicate e ispirata alla norma ISO/IEC 23894.

La valutazione tiene conto della finalità del sistema, della natura dei dati trattati, dei possibili impatti sui diritti fondamentali, dei requisiti contrattuali e del contesto di utilizzo, con particolare riferimento ai sistemi destinati alla Pubblica Amministrazione. Essa è effettuata sulla base di criteri definiti dall'organizzazione, che considerano, tra l'altro, la probabilità di accadimento e la gravità degli impatti.

Sulla base degli esiti della valutazione, PA Advice definisce e attua misure di trattamento del rischio proporzionate, selezionando controlli tecnici, organizzativi, contrattuali e formativi coerenti con il Sistema di Gestione IA e con i requisiti normativi applicabili. Tali misure sono oggetto di monitoraggio nel tempo.

I criteri di valutazione e accettazione del rischio, le modalità di selezione e applicazione dei controlli, nonché le evidenze relative ai rischi individuati e alle misure adottate, sono disciplinati nei documenti di livello 2 e 3 del SGIA, in particolare nella procedura di gestione del rischio IA e nei registri associati.

PA Advice pianifica inoltre azioni per affrontare i rischi e le opportunità individuati e ne valuta l'efficacia nel tempo, nell'ambito delle attività di monitoraggio e riesame del Sistema di Gestione IA.

4.3 Pratiche vietate

PA Advice non sviluppa, non utilizza e non promuove sistemi di IA che ricadono nelle pratiche vietate dall'AI Act, né sistemi il cui utilizzo risulti incompatibile con i principi della

presente Policy o con il Codice Etico aziendale. Le specifiche fattispecie vietate e le relative cautele sono dettagliate nelle procedure di Livello 2.

4.4 Valutazione degli impatti dei sistemi di IA

Nell'ambito dell'approccio basato sul rischio, PA Advice valuta gli impatti potenziali dei sistemi di Intelligenza Artificiale sugli individui, sui gruppi e sulla collettività, con particolare riferimento ai diritti fondamentali, alla non discriminazione, alla trasparenza e alla sicurezza.

La valutazione degli impatti è effettuata per ogni sistema di IA rientrante nell'ambito della presente Policy, in attuazione del punto 6.1.4 della norma ISO/IEC 42001:2023.

Tali valutazioni sono condotte in modo coordinato con le analisi di rischio e, qualora applicabile, con le valutazioni d'impatto previste dalla normativa in materia di protezione dei dati personali.

Per ciascun sistema di IA sono, inoltre, definite e mantenute informazioni documentate relative alle caratteristiche del sistema, alle finalità, ai dati utilizzati, ai risultati delle valutazioni e alle misure di mitigazione adottate.

5. Impegni di PA Advice

5.1 Impegni verso il personale

PA Advice si impegna a:

- mettere a disposizione del personale strumenti di IA autorizzati, sicuri e adeguati alle attività professionali;
- garantire una formazione sull'IA (AI literacy), in coerenza con quanto previsto dall'art. 4 dell'AI Act, calibrata sui ruoli e sulle responsabilità;
- definire regole chiare sull'utilizzo ammesso degli strumenti di IA, anche al fine di tutelare il personale rispetto a eventuali contestazioni;
- favorire un confronto aperto su opportunità, rischi e dilemmi etici connessi all'IA, anche tramite il Comitato IA.

5.2 Impegni verso i clienti

Nei rapporti con i propri clienti, in particolare con la Pubblica Amministrazione, PA Advice si impegna a:

- utilizzare l'IA nei progetti di consulenza nel rispetto della Policy, delle eventuali policy del cliente e del quadro normativo applicabile;
- **garantire che le funzionalità di IA integrate nei sistemi forniti ai clienti siano progettate, testate e monitorate nel rispetto della presente Policy e dei requisiti normativi applicabili, con particolare attenzione alla supervisione umana degli output prima dell'adozione di decisioni amministrative;**
- garantire trasparenza, ove rilevante, sull'impiego dell'IA nella produzione dei deliverable e nella fornitura dei servizi;
- assicurare la qualità e la verifica dei contenuti prodotti con il supporto dell'IA, mantenendo la piena responsabilità professionale dei propri consulenti;
- supportare i clienti nell'adozione consapevole e conforme dell'IA, anche attraverso servizi dedicati di assessment, governance, compliance e change management.

PA Advice assicura, inoltre, che siano rese disponibili agli utilizzatori e ai clienti informazioni adeguate sull'utilizzo dei sistemi di IA, sui limiti degli stessi e sui rischi connessi, in misura proporzionata al contesto e all'impatto.

5.3 Impegni verso i fornitori

PA Advice seleziona e gestisce i fornitori di sistemi e servizi di IA secondo criteri di affidabilità, sicurezza e conformità. Sono previste attività di due diligence e clausole

contrattuali coerenti con la presente Policy, in particolare in materia di protezione dei dati, riservatezza, gestione del rischio e responsabilità.

Con particolare riferimento ai fornitori di modelli e piattaforme di Intelligenza Artificiale, PA Advice valuta e monitora nel tempo l'affidabilità, la sicurezza e la conformità normativa dei servizi acquisiti, tenendo conto dei rischi specifici legati alla dipendenza da fornitori terzi per i componenti fondativi dei sistemi IA forniti ai clienti.

5.4 Impegni verso gli stakeholder e la collettività

PA Advice riconosce che l'adozione dell'IA da parte della Pubblica Amministrazione produce effetti rilevanti sui cittadini e sulla collettività. Per questo motivo PA Advice promuove un utilizzo dell'IA orientato al bene comune, contribuendo, ove possibile, al dibattito pubblico, alle iniziative istituzionali e allo sviluppo di buone pratiche di settore.

6. Tutela dei dati, riservatezza e proprietà intellettuale

L'utilizzo dei sistemi di IA nelle attività di PA Advice avviene nel pieno rispetto della normativa in materia di protezione dei dati personali, di tutela della riservatezza e di proprietà intellettuale, nonché degli obblighi assunti contrattualmente nei confronti dei clienti.

In particolare, **è vietato immettere in sistemi di IA non espressamente autorizzati informazioni riservate, dati personali, dati di proprietà di PA Advice e/o clienti o qualunque contenuto soggetto a vincoli di confidenzialità**. I criteri operativi di dettaglio, le valutazioni d'impatto e le regole di trattamento sono definiti nelle procedure di Livello 2 e coordinati con il DPO e con il Responsabile della Sicurezza delle Informazioni.

I contenuti generati con il supporto dell'IA sono utilizzati nel rispetto dei diritti di terzi e con adeguata tracciabilità del contributo dell'IA stessa, secondo quanto previsto dalle procedure operative.

Con riferimento specifico ai progetti con clienti della Pubblica Amministrazione, PA Advice definisce contrattualmente, ove possibile, la titolarità degli output generati con il supporto dell'IA, assicurando che i diritti sui contenuti prodotti siano chiaramente attribuiti e che l'utilizzo dell'IA nella produzione dei deliverable sia adeguatamente documentato e comunicato al cliente. Anche in assenza di specifiche previsioni contrattuali, PA Advice si impegna a garantire la massima trasparenza sull'impiego dell'IA nella produzione dei propri servizi e deliverable.

È, inoltre, definito un processo per la gestione degli incidenti relativi ai sistemi di IA, inclusa la rilevazione, la registrazione, l'analisi e, ove necessario, la comunicazione agli stakeholder e alle autorità competenti.

7. Sistema di gestione, monitoraggio e miglioramento continuo del SGIA

7.1 Documentazione del sistema di gestione

La presente Policy è il documento di vertice del SGIA di PA Advice.

Le modalità operative di attuazione sono definite nei documenti di Livello 2 (procedure e linee guida) e di Livello 3 (registri, modelli e checklist), richiamati nel documento SIST-AI-04 e gestiti in coerenza con il sistema documentale aziendale.

La gestione delle informazioni documentate avviene in coerenza con la procedura aziendale di gestione documentale, che disciplina le modalità di creazione, aggiornamento, accesso, protezione e conservazione dei documenti.

7.2 Audit e riesame della direzione

Il Sistema di Gestione dell'IA è oggetto di audit interni periodici e, ove applicabile, di audit esterni nell'ambito dei percorsi di certificazione.

Gli esiti sono portati al riesame della direzione, che ne valuta l'adeguatezza e ne definisce gli sviluppi.

[Nell'ambito del riesame della direzione è riesaminata anche la presente Policy, secondo le modalità definite al §1.6, al fine di assicurarne la continua idoneità, adeguatezza ed efficacia.](#)

7.3 Obiettivi del Sistema di Gestione IA

PA Advice definisce e mantiene nel tempo obiettivi per il Sistema di Gestione dell'Intelligenza Artificiale, coerenti con i principi e gli impegni espressi nella presente Policy.

Gli obiettivi sono stabiliti a livelli e funzioni pertinenti dell'organizzazione e tengono conto, tra l'altro, dei rischi e delle opportunità individuati, dei requisiti normativi e contrattuali applicabili, nonché delle esigenze e aspettative delle parti interessate.

Gli obiettivi sono monitorati mediante indicatori, ove opportuno misurabili, e sono soggetti a riesame periodico da parte della Direzione nell'ambito del riesame del Sistema di Gestione IA. [Gli indicatori e le relative modalità di monitoraggio sono definiti nel documento SIST-AI-06.](#)

Le modalità di definizione, aggiornamento e monitoraggio degli obiettivi, nonché le relative evidenze documentate, sono gestite nell'ambito dei documenti di livello 2 e 3 del SGIA, inclusi gli strumenti di monitoraggio, i registri e i report di audit.

7.4 Comunicazione

PA Advice assicura la comunicazione interna ed esterna relativa al Sistema di Gestione dell'Intelligenza Artificiale attraverso canali e strumenti coerenti con l'organizzazione aziendale, con la natura delle informazioni trattate e con i rischi e gli impatti associati ai sistemi di IA.

In particolare:

- la diffusione della Policy e dei relativi aggiornamenti avviene attraverso i canali aziendali, garantendone la disponibilità a tutti i destinatari e, ove pertinente, la comunicazione agli stakeholder esterni;
- le comunicazioni verso i clienti in merito all'utilizzo dei sistemi di IA sono gestite nell'ambito dei progetti e dei rapporti contrattuali, anche mediante appositi deliverable, informative o momenti di confronto dedicati;
- la segnalazione di incidenti, anomalie o criticità avviene attraverso i canali aziendali previsti (es. jira, piattaforma di whistleblowing), nel rispetto delle policy applicabili;
- le informazioni rilevanti relative ai sistemi di IA (es. stato, rischi, attività di monitoraggio) sono condivise internamente tra i ruoli coinvolti (es. AI Officer, responsabili di progetto, funzioni di controllo) nell'ambito delle attività di gestione, monitoraggio e riesame del sistema.

Le modalità operative di dettaglio, gli strumenti e le responsabilità sono definiti nei documenti di livello 2 e 3 del Sistema di Gestione IA.

7.5 Segnalazioni

Eventuali violazioni della presente Policy, malfunzionamenti significativi dei sistemi di IA o situazioni di rischio possono essere segnalati attraverso i canali previsti dalle policy aziendali, inclusi, ove pertinenti, il canale di segnalazione degli incidenti aziendali e la piattaforma di whistleblowing.

Nello specifico:

- **Dubbi o preoccupazioni relativi all'utilizzo dei sistemi di IA** (comportamenti inattesi, risultati anomali o non corretti): possono essere inoltrati all'indirizzo aiofficer@paa.it, indicando il sistema interessato e quanto osservato;
- **Incidenti** (anomalie di funzionamento del sistema, violazioni di sicurezza, perdita o trattamento non corretto di dati, eventi con impatto sulle persone): devono essere gestiti mediante apertura di una issue sulla commessa GIA in

Jira o invio di comunicazione all'indirizzo gia@paa.it, classificando la segnalazione come "IA".

- **Segnalazioni anonime o riservate** (preoccupazioni di natura etica o possibili illeciti): possono essere effettuate tramite la piattaforma di whistleblowing aziendale, accessibile dal sito istituzionale, che garantisce la tutela e l'anonimato del segnalante ai sensi del D.Lgs. 24/2023.

Le segnalazioni sono trattate nel rispetto della riservatezza e con tutela del segnalante (ove opportuno)

8. Violazioni e misure

Il mancato rispetto della presente Policy può comportare, in relazione alla gravità e alle circostanze, l'adozione di misure disciplinari nei confronti del personale dipendente, secondo quanto previsto dalla normativa vigente e dal contratto collettivo applicabile, nonché di misure contrattuali nei confronti di collaboratori, consulenti e fornitori.

Restano fermi gli eventuali profili di responsabilità civile, penale e amministrativa, ivi compresi quelli rilevanti ai sensi del D.lgs. 231/2001.