

LINEE GUIDA PER L'USO DELL'INTELLIGENZA ARTIFICIALE DEL COMUNE DI PIACENZA

Premessa

Il Comune di Piacenza riconosce nell'Intelligenza Artificiale (IA) un potenziale determinante per l'innovazione della Pubblica Amministrazione, finalizzato a incrementare l'efficienza operativa, accelerare la digitalizzazione dei servizi e migliorare sensibilmente la qualità della vita dei cittadini. In considerazione della rapidità con cui tali tecnologie evolvono e degli impatti generati, sia in termini di spinta propositiva che di profili critici, l'Amministrazione ha deliberato la costituzione di un apposito Gruppo di Lavoro con l'obiettivo di formalizzare le modalità di adozione degli strumenti di IA all'interno dell'Ente. Tale attività si articola nella duplice necessità di regolamentare l'utilizzo di queste tecnologie, garantendo un quadro di governance sicuro e responsabile, e di proporre ambiti applicativi specifici in cui le stesse possano essere efficacemente implementate per generare valore pubblico. È ferma intenzione dell'Amministrazione che l'integrazione di tali strumenti avvenga secondo principi di etica, trasparenza e inclusività, in totale coerenza con gli obiettivi di lungo termine della trasformazione digitale e con l'impegno costante a scongiurare fenomeni di "IA divide" che potrebbero ostacolare lo sviluppo dell'ecosistema urbano. A tal fine, ogni applicazione di IA adottata dal Comune di Piacenza dovrà garantire il rigoroso rispetto della normativa vigente, con particolare riferimento al Regolamento Generale sulla Protezione dei Dati (GDPR), e al Regolamento (UE) 2024/1689 (AI Act) e alle Linee Guida AgID, assicurando la massima tutela dei diritti dei cittadini, la sicurezza dei dati e il mantenimento della supervisione umana su ogni processo decisionale critico.

Principi Fondamentali

L'utilizzo dell'IA da parte del Comune di Piacenza si basa sui seguenti principi inderogabili:

- **Umanesimo Digitale:** L'Intelligenza Artificiale (IA) è al servizio della persona e non sostituisce il valore del contatto umano, ma lo potenzia nel rispetto della dignità e dei diritti fondamentali.
- **Trasparenza:** Il Comune si impegna a esplicitare l'uso di Intelligenza Artificiale (IA) all'interno di processi, di sistemi conversazionali in ambito pubblico, riportando in modo onesto i limiti dello strumento impiegato ed esplicando quando l'Intelligenza Artificiale (IA) è utilizzata a supporto della redazione di testi.
- **Spiegabilità:** Il Comune si impegna ad illustrare le logiche di funzionamento e i criteri decisionali dei sistemi di IA utilizzati, in particolare quando incidono su diritti o aspettative dei cittadini.
- **Equità e Non Discriminazione:** I sistemi di Intelligenza Artificiale (IA) non devono generare o amplificare disuguaglianze e verranno sottoposti a valutazioni d'impatto etico e sociale per garantire un accesso equo ai servizi.

- **Sicurezza e Protezione dei Dati:** Deve essere garantita la massima tutela delle informazioni, nel pieno rispetto della normativa sulla privacy e sulla cybersecurity, limitando la raccolta dei dati personali allo stretto necessario.
- **Responsabilità:** chiunque utilizzi strumenti di Intelligenza Artificiale (IA) è personalmente responsabile dell'uso che ne fa. Ogni contenuto generato mediante Intelligenza Artificiale (IA) deve essere rivisto prima della sua diffusione/utilizzo.
- **Controllo Umano (Human-in-the-loop):** Le decisioni critiche non verranno mai delegate esclusivamente all'automazione algoritmica; resteranno sempre sotto la supervisione e la potenziale revisione di un operatore pubblico. Gli output generati da strumenti di IA devono essere sempre sottoposti a verifica e validazione da parte di coloro che se ne avvalgono e i contenuti generati da Intelligenza Artificiale (IA) devono sempre derivare da una valutazione umana consapevole. Spetta agli utilizzatori assicurarsi che le informazioni siano corrette, aggiornate e coerenti con le fonti ufficiali.

Definizioni

Concetti Base: Definizioni e Differenze

1. **Sistema di Intelligenza Artificiale (IA):** È l'unione tra un modello (l'algoritmo) e il software che lo rende utilizzabile. È l'interfaccia con cui l'utente dialoga. Esempio: Gemini per Google Workspace, usato come assistente in un ente, è un sistema fornito da Google che include sia l'interfaccia (dentro Gmail o Docs) sia il modello.
2. **Modello di intelligenza artificiale:** È il "motore" o l'algoritmo che elabora i dati per creare una risposta. Non è utilizzabile da solo, ma deve essere integrato in una piattaforma. Esempio: Gemini 1.5 Pro è un modello di Google. Può essere integrato in vari sistemi: nella chat web, nelle app di Workspace o in software personalizzati.
3. **IA generativa:** Una tipologia di IA capace di creare contenuti nuovi (testi, immagini, suoni) invece di limitarsi a classificare dati esistenti. Funziona su basi probabilistiche: non "capisce" davvero il senso, ma prevede la parola successiva più probabile.
4. **LLM (Large Language Model):** Modello linguistico addestrato su enormi quantità di testo per comprendere e generare il linguaggio umano. Esempio: Gemini è un LLM; avendo letto milioni di documenti, può scrivere bozze di atti amministrativi o riassumere lunghe relazioni in italiano.

Ruoli e Responsabilità

5. **Deployer:** È l'ente (es. un Comune) che utilizza concretamente il sistema di IA nei propri uffici. Ha la responsabilità di decidere come usarlo e di controllare che i risultati siano corretti e trasparenti.
6. **Provider:** È il soggetto che sviluppa e mette in commercio il sistema. È responsabile della sicurezza tecnica e della conformità legale. Esempio: Se un ente acquista licenze Google Workspace per i dipendenti, Google è il provider, mentre l'ente è il deployer.

Funzionamento Operativo

7. **Prompt:** È il comando o l'istruzione che l'utente scrive per attivare l'IA. Esempio: Scrivere nel pannello laterale di Google Docs "Sintetizza questo verbale in 5 punti chiave" è un prompt.
8. **Output generato:** È il risultato (testo, tabella, codice) prodotto dall'IA. Nella PA, l'output non è mai un atto definitivo: deve essere sempre validato da un funzionario.
9. **Token:** Le unità di misura del testo elaborate dall'IA (1 token $\approx$ 3-4 caratteri). I sistemi hanno limiti di token (finestra di contesto): se il documento è troppo lungo, l'IA potrebbe ignorarne delle parti.
10. **Prompt engineering:** La capacità di scrivere comandi strategici e precisi per ottenere risultati migliori (es. specificare il tono, la lunghezza o il destinatario di una mail in Gmail).
11. **Training set:** L'insieme di dati usati per "istruire" il modello originario. Se i dati di partenza sono scarsi sul diritto amministrativo italiano, l'IA potrebbe essere meno precisa.

Tipologie e Strumenti

12. **Modello conversazionale:** Un'IA progettata per dialogare in modo naturale, mantenendo il filo del discorso tra una domanda e l'altra.
13. **Chatbot AI:** Il software che simula la conversazione.* *Esempio:* Gemini (Google), ma anche altri come Copilot (Microsoft) o Claude (Anthropic).
14. **Multimodale:** Un sistema che gestisce formati diversi contemporaneamente. Esempio: Caricare su Google Drive la foto di un documento cartaceo e chiedere a Gemini di trasformarlo in una tabella digitale e riassumerlo.
15. **Agente AI:** Un'entità digitale che svolge compiti complessi in autonomia (es. cercare dati su Drive, scrivere una bozza e preparare la mail di invio senza interventi continui).

Aspetti Tecnici Avanzati

16. **API (Application Programming Interface):** Il "ponte" tecnico che permette di collegare l'IA di Google ai software già usati dall'ente, senza dover aprire il browser.
17. **Fine-tuning:** Il processo di specializzazione di un modello su dati specifici di un ente per renderlo un "esperto" di quel settore.
18. **RAG (Retrieval-Augmented Generation):** Tecnica che permette all'IA di rispondere usando documenti aggiornati e sicuri presenti nei database dell'ente (es. i file salvati su Google Drive), riducendo il rischio di errori.

Rischi e Governance

19. **Allucinazione:** Quando l'IA inventa fatti o leggi inesistenti presentandoli come veri. È il rischio principale per chi scrive atti amministrativi.
20. **Shadow AI:** L'uso di IA (es. la versione gratuita di Gemini o ChatGPT) da parte dei dipendenti senza che l'ente ne abbia autorizzato l'uso o stabilito regole di sicurezza.
21. **Supervisione umana:** Il controllo obbligatorio da parte di una persona su ogni output dell'IA prima che diventi operativo.
22. **Explainability (Spiegabilità):** La capacità dell'IA di mostrare i passaggi logici e le fonti (es. citando i documenti di Drive usati) per arrivare a una conclusione.

23. **Tracciabilità:** La possibilità di documentare l'uso dell'IA nel processo decisionale per garantire che l'azione amministrativa sia trasparente.
24. **AGI (Intelligenza Artificiale Generale):** Un'IA futura capace di eguagliare l'intelligenza umana in ogni campo. Oggi è ancora un concetto teorico.

Ambito di applicazione

Le presenti Linee Guida si applicano a tutti i sistemi di Intelligenza Artificiale (IA) utilizzati dall'Ente, sia in forma diretta che per il tramite di soggetti esterni, partner o fornitori. L'ambito di applicazione comprende tutte le fasi del ciclo di vita dei sistemi di Intelligenza Artificiale (IA), incluse:

- la selezione e acquisizione;
- la progettazione, sviluppo e sperimentazione;
- l'utilizzo operativo e la manutenzione evolutiva;
- la dismissione o sostituzione.

Le disposizioni delle seguenti Linee Guida si applicano, in particolare:

- ai servizi digitali rivolti al cittadino o alle imprese;
- ai processi interni automatizzati di supporto amministrativo, tecnico o decisionale.

Classificazione dei sistemi in base al rischio

Il Comune di Piacenza adotta i criteri di classificazione dei sistemi mediante una classificazione del rischio; come previsto dal Regolamento (UE) 2024/1689 (AI Act) per i sistemi di Intelligenza Artificiale (IA):

- **Sistemi Inaccettabili:** Pratiche vietate ex art. 5 del Regolamento sopra citato.
- **Sistemi ad Alto Rischio:** Applicazioni soggette alle prescrizioni del Titolo III, richiedenti FRIA, DPIA e autorizzazione dirigenziale.
- **Sistemi a Rischio Limitato:** Applicazioni interattive soggette a doveri di informativa e trasparenza.
- **Sistemi a Rischio Minimo:** Strumenti di supporto generico il cui uso è ammesso previo monitoraggio dell'Ente.

Divieti

In ossequio al principio di precauzione e in conformità con i principi fondamentali sopra citati, oltre che all'art. 5 del Regolamento (UE) 2024/1689 (AI Act), il Comune di Piacenza, proibisce tassativamente l'adozione di sistemi di IA a rischio inaccettabile. Nello specifico, è vietato l'impiego di tecnologie che possano condizionare subdolamente la volontà dell'individuo, sfruttare le fragilità di categorie protette (minori, anziani, disabili) o implementare meccanismi di valutazione sociale (social scoring) finalizzati a trattamenti discriminatori o sproporzionati.

Referenti e competenze

La responsabilità dell'applicazione delle presenti Linee Guida è ripartita secondo le seguenti competenze: il Responsabile della Transizione Digitale (RTD) funge da cardine operativo per

l'intero ciclo di vita dei sistemi (dall'adozione al monitoraggio); il Responsabile della protezione dei dati (DPO) vigila sulla coerenza con il GDPR e sulla tutela dei diritti degli interessati; il Direttore Generale svolge compiti di coordinamento organizzativo; il Responsabile Anticorruzione svolge compiti di vigilanza rispetto alla prevenzione di fenomeni di illegalità, il Dirigenti di Settore e i Responsabili dei Servizi, infine, garantiscono l'osservanza delle presenti norme nelle attività quotidiane dei rispettivi uffici, assicurando che l'Intelligenza Artificiale (IA) sia utilizzata in conformità ai fini istituzionali.

Costituzione Gruppo di Lavoro

Il Responsabile per la trasformazione digitale (RTD) ha istituito, con atto formale, un Gruppo di lavoro interdisciplinare, finalizzato alla valutazione, classificazione e revisione dei sistemi di Intelligenza Artificiale (IA), nonché al supporto tecnico e giuridico per le attività previste dalle presenti Linee Guida.

Principio di responsabilità umana

In linea con quanto definito nell'ambito di applicazione, l'Ente assicura che ogni provvedimento o risultato generato da sistemi di Intelligenza Artificiale (IA) avente effetti su terzi rispetti i canoni di trasparenza, documentabilità e controllo. Nello specifico, deve essere garantita la comprensibilità dei criteri decisionali e delle fonti, l'archiviazione sistematica dell'iter procedurale e, in ogni caso, una revisione critica da parte di un operatore umano che ne assuma la paternità giuridica. È fatto divieto di delegare in modo totale e automatizzato le funzioni deliberative che la legge riserva esclusivamente alla dirigenza o agli organi politici.

Valutazioni preliminari obbligatorie

Prima dell'adozione, acquisizione o utilizzo di un sistema di Intelligenza Artificiale (IA), l'Ente è tenuto a svolgere una valutazione preliminare articolata, comprensiva di:

- Classificazione del rischio, sulla base dei criteri di cui all'Allegato A;
- FRIA (Fundamental Rights Impact Assessment), obbligatoria per tutti i sistemi di Intelligenza Artificiale (IA) classificati ad alto rischio, redatta ai sensi dell'art. 27 del Regolamento (UE) 2024/1689;
- DPIA (Data Protection Impact Assessment), ove richiesto ai sensi dell'art. 35 del GDPR e previa consultazione del DPO;
- Valutazione trasversale c.d. AIIA, condotta congiuntamente dal RTD e dal DPO, finalizzata a garantire la compatibilità del sistema con i principi di proporzionalità, minimizzazione dei dati, sicurezza e trasparenza.

Nei casi in cui il sistema di Intelligenza Artificiale (IA) incida su ambiti particolarmente sensibili, quali:

- servizi sociali
- istruzione
- fiscalità locale
- mobilità
- edilizia pubblica
- sanità,
- sicurezza urbana o procedimenti sanzionatori

la FRIA deve essere pubblicata, in formato accessibile, nella sezione "Intelligenza Artificiale nell'Ente" del sito istituzionale. Le valutazioni preliminari devono essere rivalutate in caso di modifiche sostanziali del sistema, aggiornamenti software significativi, estensione delle funzionalità o mutamenti del contesto giuridico o organizzativo di utilizzo.

Autorizzazione formale

L'impiego di sistemi di Intelligenza Artificiale (IA) classificati ad alto rischio dal gruppo di lavoro è consentito esclusivamente previa adozione di un provvedimento autorizzativo formale.

L'iter prevede: l'elaborazione dell'istruttoria tecnica da parte del RTD insieme al gruppo di lavoro, basata sulle analisi di impatto (FRIA e DPIA); l'ottenimento del parere obbligatorio e vincolante del DPO in materia di conformità dei dati; infine, l'emanazione di una determinazione dirigenziale da parte del dirigente del Servizio Competente in materia di Sistemi Informativi, che specifichi le ragioni del ricorso alla tecnologia, le modalità d'uso, la validità temporale e le necessarie precauzioni per ridurre i rischi.

Soluzioni di Intelligenza Artificiale

In fase di affidamento o contrattualizzazione di soluzioni di Intelligenza Artificiale (IA), l'Ente promuove la collaborazione con i fornitori per garantire un impiego sicuro e trasparente della tecnologia. A tal fine, negli atti di gara o nei contratti, si prevede che il fornitore si impegni a:

- **Assicurare il rispetto del quadro normativo vigente**, con particolare riferimento al Regolamento (UE) 2024/1689 (AI Act) e alla disciplina sulla protezione dei dati personali (GDPR), seguendo le indicazioni fornite dalle Linee guida AgID;
- **Mettere a disposizione le informazioni necessarie** (documentazione tecnica e funzionale) per consentire all'Ente di inquadrare correttamente il sistema e di completare le valutazioni di impatto richieste dalla legge (FRIA e DPIA);
- **Fornire il supporto necessario** per le attività di verifica e monitoraggio che l'Ente dovesse ritenere opportune, anche dopo la messa in funzione del sistema, per assicurarne il corretto funzionamento nel tempo;
- **Dichiarare la propria responsabilità** per eventuali difformità o malfunzionamenti del sistema che possano generare output discriminatori o violazioni di legge, impegnandosi a collaborare con l'Ente per la risoluzione di eventuali criticità.

Registro dei sistemi di intelligenza artificiale

Al fine di garantire la massima trasparenza e tracciabilità, è istituito il Registro dei sistemi di Intelligenza Artificiale (IA) dell'Ente. Tale registro documenta per ogni software: la natura e lo scopo, la classe di rischio assegnata, i risultati delle analisi d'impatto e le precauzioni operative adottate. Il documento, aggiornato periodicamente, funge da strumento di monitoraggio interno ed è messo a disposizione della Direzione Generale per la supervisione annuale sulle tecnologie in uso.

Divieto Uso Strumenti non Autorizzati e Shadow AI

L'utilizzo di strumenti di Intelligenza Artificiale gratuiti, a uso personale o comunque non esplicitamente approvati da parte dell'Ente, configura il fenomeno della Shadow AI. L'utilizzo di tali strumenti è da ritenersi non autorizzato.

Monitoraggio e audit

Al fine di assicurare la persistenza dei requisiti di sicurezza e legittimità, il RTD — d'intesa con il DPO — coordina un'attività di revisione annuale (audit) su tutte le soluzioni di Intelligenza Artificiale (IA) in esercizio. Tale verifica è volta ad accertare la tenuta normativa del sistema, l'assenza di derive discriminatorie o pregiudizi algoritmici (bias), nonché l'efficacia dei presidi tecnici e delle misure di mitigazione. Gli esiti del monitoraggio sono formalizzati in un verbale trasmesso al Responsabile Anticorruzione dell'Ente per le valutazioni di competenza e l'eventuale adozione di misure correttive.

Trasparenza verso l'utenza

Per ogni sistema attivo di Intelligenza Artificiale (IA) che incida, anche indirettamente, sull'erogazione di servizi pubblici o sull'interazione con i cittadini, l'Ente garantisce adeguata informazione e trasparenza. In particolare, l'Ente:

- pubblica sul sito istituzionale un elenco aggiornato dei sistemi di IA in uso, con indicazione della finalità e del livello di rischio;
- mette a disposizione schede informative sintetiche sul funzionamento e sugli impatti dei sistemi adottati;
- attiva canali dedicati per la raccolta di osservazioni, segnalazioni, richieste di accesso o reclami da parte degli utenti.

Formazione del personale

Al fine di garantire un'interazione consapevole e sicura con le nuove tecnologie, l'Ente promuove un piano di sviluppo delle competenze digitali rivolto al proprio personale. Tale piano si articola in: sessioni specifiche per gli addetti ai sistemi di IA, aggiornamenti continui sulle novità tecnico-giuridiche del settore e iniziative di sensibilizzazione aperte a tutta la struttura, focalizzate sull'impatto etico e sulla salvaguardia dei diritti fondamentali nell'uso degli algoritmi.

Partecipazione e coinvolgimento civico

L'Ente si propone di coinvolgere gli stakeholders nei processi che porteranno all'adozione di tecnologie basate su IA che abbiano un impatto su cittadini e imprese tramite:

- Forum cittadini e imprese sull'IA per ascolto e confronto;
- Campagne di alfabetizzazione digitale nelle biblioteche e nei quartieri

Misure correttive e segnalazioni

In caso di utilizzo scorretto, improprio, non autorizzato o non conforme di un sistema di Intelligenza Artificiale (IA), l'Ente adotta tempestivamente le misure necessarie finalizzate a porre in essere correzioni o sospensione della funzionalità individuata. Il personale dell'Ente, nonché collaboratori e fornitori, possono segnalare in forma riservata o anonima eventuali utilizzi distorti, discriminatori o illeciti di sistemi di IA, tramite i canali interni previsti dalla normativa vigente in materia di segnalazioni (D.lgs. 10 marzo 2023, n. 24).

Le segnalazioni devono essere:

- tempestivamente valutate dal RTD, anche con il supporto del DPO
- tutelate sotto il profilo della riservatezza

Aggiornamenti e revisioni delle Linee Guida

Le presenti Linee Guida, sono soggette a revisione almeno annuale, da effettuarsi in occasione:

- dell'aggiornamento del Piano Triennale per l'Informatica nella Pubblica Amministrazione;
- della definizione del PIAO (Piano Integrato di Attività e Organizzazione);
- dell'entrata in vigore di nuove disposizioni normative, regolamentari o Linee Guida in materia di IA, digitalizzazione o protezione dei dati.

Le proposte di aggiornamento possono essere formulate dal RTD, dal DPO, della Direzione Generale o su iniziativa degli Organi dell'Ente, anche a seguito di audit, segnalazioni o evoluzioni tecniche rilevanti.

Entrata in vigore e ambito temporale di applicazione

Le presenti Linee Guida entrano in vigore a decorrere dalla data della loro adozione, mediante apposito atto dell'organo competente. Le sue disposizioni si applicano sia ai sistemi di Intelligenza Artificiale (IA) già attivi o in uso presso l'Ente, sia a quelli di futura acquisizione, sviluppo o implementazione.

Allegati operativi

– [Allegato A – Registro dei sistemi di IA](#)