



CITTÀ DI VITTORIA

(Libero Consorzio Comunale di Ragusa)

Direzione Risorse Umane e Servizi Informatici

OGGETTO: ALLEGATO “A” - Approvazione delle “Linee Guida per l'utilizzo responsabile dei sistemi di Intelligenza Artificiale nel Comune di Vittoria”.

ALLEGATO “A”

Art. 1 – Oggetto e finalità

1. Le presenti Linee Guida disciplinano l'utilizzo responsabile, consapevole, sicuro e conforme alla normativa vigente dei sistemi e delle funzionalità di Intelligenza Artificiale (IA) da parte del Comune di Vittoria.

2. Le Linee Guida perseguono le seguenti finalità:

- a) favorire un utilizzo dell'IA orientato al miglioramento della qualità, dell'efficienza e della tempestività dell'azione amministrativa;
- b) assicurare il rispetto dei diritti e delle libertà fondamentali delle persone;
- c) tutelare i dati personali, le informazioni riservate e il segreto d'ufficio;
- d) garantire la responsabilità umana sulle attività amministrative e sulle decisioni adottate dall'Ente;
- e) prevenire utilizzi impropri, non autorizzati o non sicuri dei sistemi di IA;
- f) promuovere la conoscenza dei rischi, dei limiti e delle potenzialità dell'IA tra il personale dell'Ente;
- g) assicurare il progressivo adeguamento dell'organizzazione agli obblighi derivanti dalla normativa europea e nazionale in materia di IA.

3. Le presenti Linee Guida costituiscono il quadro organizzativo e operativo interno dell'Ente per la gestione e l'utilizzo dei sistemi di IA e devono essere applicate in coerenza con la normativa europea e nazionale vigente, con le disposizioni dell'Ente in materia di sicurezza informatica, protezione dei dati personali, gestione documentale, trasparenza, procedimento amministrativo e con gli eventuali ulteriori atti di indirizzo emanati dalle autorità competenti.

Art. 2 – Ambito di applicazione

1. Le presenti Linee Guida si applicano al personale dipendente del Comune di Vittoria, ai dirigenti e ai responsabili delle strutture organizzative, nonché, per quanto compatibile con la natura del rapporto e con gli obblighi contrattualmente assunti, ai collaboratori, consulenti, tirocinanti e altri soggetti che utilizzino sistemi di IA nello svolgimento di attività per conto dell'Ente.
2. Le disposizioni si applicano sia ai sistemi di IA utilizzati direttamente dal personale, sia alle funzionalità di IA integrate in applicativi, piattaforme, servizi cloud, sistemi documentali, gestionali o altri strumenti informatici utilizzati dall'Ente.
3. I dirigenti e i responsabili delle strutture organizzative sono tenuti, nell'ambito delle rispettive competenze, a vigilare sul rispetto delle presenti Linee Guida.

Art. 3 – Principi generali

1. L'utilizzo dell'IA nell'Amministrazione deve essere improntato ai seguenti principi:
 - a) **legalità e conformità normativa**, assicurando il rispetto della normativa europea, nazionale e regionale applicabile;
 - b) **centralità della persona**, garantendo che l'utilizzo della tecnologia sia orientato al perseguimento dell'interesse pubblico e alla tutela dei diritti delle persone;
 - c) **responsabilità**, assicurando che sia sempre individuabile il soggetto responsabile dell'attività amministrativa nella quale il sistema di IA è utilizzato;
 - d) **controllo umano**, evitando che un sistema di IA sostituisca autonomamente il soggetto competente nell'adozione di decisioni amministrative;
 - e) **proporzionalità**, utilizzando sistemi e funzionalità di IA in misura adeguata alle finalità perseguite e ai rischi connessi;
 - f) **sicurezza**, adottando misure adeguate a prevenire perdita, divulgazione, alterazione o uso improprio delle informazioni;
 - g) **protezione dei dati personali**, nel rispetto del Regolamento (UE) 2016/679 e della normativa nazionale vigente;
 - h) **trasparenza e tracciabilità**, nei casi e nei limiti previsti dalla normativa applicabile;
 - i) **accuratezza e affidabilità**, attraverso la verifica degli output prodotti dai sistemi;
 - j) **non discriminazione**, prevenendo, per quanto ragionevolmente individuabile, effetti discriminatori derivanti dall'utilizzo dei sistemi;
 - k) **formazione e alfabetizzazione**, assicurando al personale competenze adeguate al ruolo svolto e al livello di utilizzo dell'IA.

Art. 4 – Responsabilità e controllo umano

1. L'utilizzo di un sistema di IA costituisce uno strumento di supporto all'attività dell'Amministrazione e non determina, di per sé, il trasferimento della responsabilità amministrativa, tecnica o decisionale al sistema.
2. Gli output prodotti dall'IA devono essere considerati, salvo diversa specifica disciplina, come risultati elaborativi che necessitano di valutazione da parte dell'operatore.
3. Il dipendente che utilizza un sistema di IA è responsabile della verifica dell'output nella misura corrispondente alle funzioni svolte e alla rilevanza dell'attività interessata.
4. Gli atti, i provvedimenti e le decisioni amministrative rimangono nella responsabilità del soggetto competente secondo l'ordinamento dell'Ente.
5. L'utilizzo dell'IA non esonera il dipendente dall'obbligo di verificare:

- a) correttezza dei dati e delle informazioni;
- b) attendibilità delle fonti;
- c) conformità alla normativa vigente;
- d) coerenza dell'output con il procedimento amministrativo;
- e) eventuali errori, omissioni, distorsioni o contenuti inventati dal sistema.

Art. 5 – Utilizzi ordinariamente consentiti

1. Nel rispetto delle presenti Linee Guida, l'IA può essere utilizzata come strumento di supporto, tra l'altro, per:

- a) predisposizione di bozze e testi non definitivi;
- b) revisione linguistica, ortografica e stilistica;
- c) traduzione e semplificazione linguistica;
- d) sintesi di documenti non riservati;
- e) classificazione o organizzazione preliminare di informazioni non personali o già pubblicamente disponibili;
- f) supporto alla ricerca di informazioni e alla consultazione di fonti, fermo restando l'obbligo di verifica delle fonti;
- g) elaborazione di schemi, prospetti, checklist e materiali di lavoro;
- h) supporto alla programmazione e all'organizzazione interna;
- i) supporto alla produzione di materiali informativi e comunicativi, con verifica e validazione umana;
- j) attività di analisi preliminare e simulazione che non producano automaticamente effetti giuridici nei confronti di persone fisiche o giuridiche.

2. L'elenco di cui al comma 1 ha carattere esemplificativo e non esonera l'utilizzatore dalla verifica della compatibilità dello specifico impiego con la normativa vigente e con le presenti Linee Guida.

Art. 6 – Utilizzi soggetti a preventiva valutazione

1. Prima dell'utilizzo stabile o sistematico di un sistema di IA deve essere effettuata una valutazione preliminare, proporzionata alla natura, alle finalità e ai rischi dell'impiego, quando il sistema:

- a) tratta dati personali non pubblicamente disponibili;
- b) tratta dati appartenenti a categorie particolari o dati relativi a condanne penali e reati;
- c) tratta informazioni coperte da segreto d'ufficio o comunque riservate;
- d) è destinato a supportare decisioni che possono incidere significativamente sui diritti o sugli interessi delle persone;
- e) effettua attività di profilazione;
- f) interagisce direttamente con cittadini o utenti nell'ambito di servizi pubblici;
- g) è destinato a essere integrato in procedimenti amministrativi dell'Ente;
- h) può rientrare nella categoria dei sistemi ad alto rischio ai sensi dell'AI Act;
- i) è acquisito dall'Ente attraverso un contratto di fornitura, appalto, concessione o altro rapporto con un soggetto esterno;
- j) è integrato in applicativi, piattaforme, servizi cloud o altri strumenti informatici già utilizzati dall'Ente e introduce funzionalità di IA suscettibili di incidere sul trattamento dei dati, sulla sicurezza, sui procedimenti amministrativi o sui diritti delle persone.

2. La valutazione preliminare ha lo scopo di individuare, in relazione allo specifico caso d'uso:

- a) la finalità e il contesto di utilizzo;

- b) la tipologia e le caratteristiche del sistema;
- c) le categorie di dati e informazioni trattate;
- d) i soggetti interessati dall'utilizzo;
- e) il livello di autonomia del sistema;
- f) i rischi per la sicurezza, la protezione dei dati personali e i diritti e le libertà delle persone;
- g) l'eventuale riconducibilità del sistema alle categorie previste dal Regolamento (UE) 2024/1689;
- h) le misure di supervisione e controllo umano;
- i) gli eventuali obblighi del Comune in qualità di deployer;
- j) gli eventuali adempimenti in materia di protezione dei dati personali, compresa, ove necessaria, valutazione d'impatto ai sensi dell'articolo 35 del Regolamento (UE) 2016/679;
- k) l'eventuale necessità di una valutazione d'impatto sui diritti fondamentali ai sensi dell'articolo 27 Regolamento (UE) 2024/1689;
- l) le misure tecniche, organizzative e contrattuali necessarie per l'utilizzo del sistema.

3. La valutazione preliminare è effettuata secondo le modalità definite dall'Ente e documentata mediante apposita scheda di valutazione del caso d'uso IA.

4. La valutazione è effettuata dalla struttura competente per l'attività o il procedimento interessato, con il coinvolgimento, ove necessario in relazione alla natura del caso d'uso, del Responsabile per la Transizione al Digitale (RTD), del Responsabile della Protezione dei Dati (DPO), del responsabile della sicurezza informatica e delle ulteriori strutture o professionalità competenti.

5. L'esito della valutazione preliminare è registrato nel Registro interno dei sistemi e dei casi d'uso di IA di cui all'articolo 15, secondo le modalità definite dall'Ente.

6. L'utilizzo del sistema non può essere avviato, ove previsto dalle presenti Linee Guida o dalla normativa applicabile, prima del completamento delle valutazioni e degli adempimenti necessari.

Art. 7 – Protezione dei dati personali

1. L'utilizzo di sistemi di IA che comporti un trattamento di dati personali deve avvenire nel pieno rispetto del Regolamento (UE) 2016/679, del decreto legislativo 30 giugno 2003, n. 196, come modificato e integrato, e della restante normativa applicabile in materia di protezione dei dati personali.

2. È vietato inserire in sistemi di IA non autorizzati dall'Ente o comunque non previamente sottoposti alle verifiche previste dalle presenti Linee Guida:

- a) dati personali dei cittadini o degli utenti;
- b) dati relativi a procedimenti amministrativi non pubblici;
- c) dati sanitari;
- d) dati giudiziari;
- e) dati relativi a minori;
- f) credenziali, chiavi di accesso o informazioni di sicurezza;
- g) informazioni coperte da segreto d'ufficio;
- h) informazioni riservate relative a dipendenti, fornitori, imprese o procedimenti;
- i) qualsiasi altra informazione la cui divulgazione possa arrecare pregiudizio all'Ente o agli interessati.

3. Il divieto di cui al comma 2 si applica in particolare ai sistemi di IA generativa accessibili tramite servizi pubblici o commerciali quando l'Ente non abbia preventivamente verificato, secondo la natura del servizio, le condizioni di trattamento dei dati, le garanzie contrattuali e organizzative, le modalità di conservazione, cancellazione, riutilizzo e trasferimento dei dati e le ulteriori condizioni di sicurezza applicabili.

4. L'eventuale utilizzo di dati personali deve essere preceduto dalle verifiche previste dalla normativa in materia di protezione dei dati personali e dalle disposizioni interne dell'Ente, comprese, ove necessarie, la valutazione d'impatto sulla protezione dei dati e la consultazione del DPO.

5. L'anonimizzazione o la pseudonimizzazione dei dati non escludono, ove pertinenti, la necessità di verificare l'effettiva efficacia delle misure adottate, il rischio di re-identificazione e la possibilità che le informazioni residue consentano comunque di individuare direttamente o indirettamente una persona.

Art. 8 – Riservatezza e segreto d'ufficio

1. Il dipendente mantiene nei confronti dei sistemi di IA gli stessi obblighi di riservatezza previsti nei confronti di qualsiasi soggetto esterno all'Amministrazione.

2. Non possono essere inserite in un sistema di IA non espressamente autorizzato informazioni soggette a:

- a) segreto d'ufficio;
- b) obblighi di riservatezza;
- c) segreto professionale;
- d) vincoli di sicurezza;
- e) tutela di procedimenti amministrativi, giudiziari o disciplinari non pubblici.

3. L'eventuale anonimizzazione o pseudonimizzazione dei dati non esclude l'obbligo di valutare preventivamente il rischio di re-identificazione o di divulgazione di informazioni riservate.

Art. 9 – Verifica degli output e affidabilità delle informazioni

1. Gli output prodotti dai sistemi di IA non possono essere considerati, per il solo fatto di essere stati generati automaticamente, veri, completi, aggiornati o conformi alla normativa.

2. Prima di utilizzare un output nell'attività amministrativa, l'operatore verifica, in relazione alla rilevanza dell'utilizzo:

- a) correttezza fattuale;
- b) completezza;
- c) aggiornamento;
- d) attendibilità delle fonti;
- e) eventuali citazioni normative o giurisprudenziali;
- f) assenza di contenuti discriminatori o impropri;
- g) coerenza con gli atti e la documentazione del procedimento.

3. Particolare attenzione deve essere prestata alle cosiddette “allucinazioni”, consistenti nella generazione di informazioni inesistenti, inesatte o prive di adeguato fondamento.

4. Nessun riferimento normativo, giurisprudenziale, dato statistico o informazione rilevante ai fini di un procedimento amministrativo deve essere utilizzato esclusivamente sulla base dell'output di un sistema di IA.

Art. 10 – Atti amministrativi e decisioni

1. L'IA può essere utilizzata come strumento di supporto alla predisposizione di bozze di atti amministrativi, relazioni, comunicazioni e documenti di lavoro.

2. L'output dell'IA non costituisce di per sé un atto amministrativo e non può essere automaticamente sottoscritto o adottato senza preventiva verifica e validazione da parte del soggetto competente.
3. È vietato utilizzare sistemi di IA in modo tale da delegare integralmente al sistema:
- a) l'istruttoria di un procedimento senza controllo umano;
 - b) la valutazione definitiva di una posizione individuale;
 - c) l'adozione di una decisione amministrativa;
 - d) la determinazione automatica di diritti, obblighi, benefici o sanzioni nei confronti di persone, salvo che ciò sia specificamente consentito e disciplinato dalla normativa applicabile e siano state adottate tutte le necessarie garanzie.
4. Nei casi di particolare rilevanza per i diritti e gli interessi degli interessati, deve essere assicurato un livello di controllo umano adeguato alla natura e ai rischi dell'attività.

Art. 11 – Sistemi di IA ad alto rischio

1. L'Ente presta particolare attenzione ai sistemi di IA che possono rientrare nelle categorie di sistemi ad alto rischio previste dal Regolamento (UE) 2024/1689.
2. La classificazione di un sistema come sistema di IA ad alto rischio deve essere effettuata con riferimento allo specifico sistema, alla sua finalità prevista, al contesto concreto di utilizzo e ai criteri stabiliti dal Regolamento (UE) 2024/1689, tenendo conto della normativa e degli atti applicabili successivamente intervenuti.
3. Qualora un sistema utilizzato o da utilizzare dall'Ente possa rientrare nelle categorie di cui all'articolo 6 del Regolamento (UE) 2024/1689, la struttura competente procede a una specifica valutazione preliminare, con il coinvolgimento delle figure competenti.
4. La valutazione di cui al comma 3 deve considerare, almeno:
- a) finalità e contesto di utilizzo;
 - b) soggetti interessati;
 - c) impatto sui diritti fondamentali;
 - d) trattamento dei dati personali;
 - e) livello di autonomia del sistema;
 - f) possibilità di controllo e intervento umano;
 - g) obblighi posti dall'AI Act a carico del deployer;
 - h) obblighi e responsabilità del fornitore;
 - i) documentazione e tracciabilità;
 - j) misure di sicurezza;
 - k) eventuali obblighi di registrazione, monitoraggio e valutazione.
 - l) eventuali obblighi di informazione nei confronti degli interessati;
 - m) eventuali obblighi di valutazione d'impatto sulla protezione dei dati personali;
 - n) eventuali obblighi di valutazione d'impatto sui diritti fondamentali.
5. Qualora il Comune utilizzi un sistema di IA ad alto rischio in qualità di deployer, sono adottate le misure tecniche e organizzative necessarie per assicurare il rispetto degli obblighi applicabili, comprese, ove pertinenti:
- a) la designazione delle persone incaricate della supervisione umana, dotate della competenza, formazione e autorità necessarie;
 - b) il monitoraggio del funzionamento del sistema;

- c) la verifica della qualità e della pertinenza dei dati di input, nella misura in cui essi siano sotto il controllo dell'Ente;
- d) la conservazione dei log nella misura prevista dalla normativa applicabile e nei limiti consentiti dalla disciplina in materia di protezione dei dati personali;
- e) la gestione degli incidenti e delle anomalie;
- f) l'adozione delle misure necessarie per interrompere o sospendere l'utilizzo del sistema quando ne ricorrano i presupposti;
- g) gli ulteriori adempimenti previsti dalla normativa europea e nazionale.

6. Nei casi previsti dall'articolo 27 del Regolamento (UE) 2024/1689, prima del primo utilizzo del sistema deve essere effettuata la valutazione d'impatto sui diritti fondamentali, secondo le modalità previste dalla normativa applicabile.

7. La valutazione d'impatto sui diritti fondamentali è coordinata, ove pertinente, con la valutazione d'impatto sulla protezione dei dati personali prevista dall'articolo 35 del Regolamento (UE) 2016/679, evitando duplicazioni e assicurando il raccordo tra i relativi adempimenti.

8. Qualora la normativa applicabile preveda obblighi di registrazione del sistema o del relativo utilizzo, tali obblighi devono essere assolti prima dell'avvio dell'utilizzo nei casi e secondo le modalità previste dalla normativa vigente.

9. Nessun sistema potenzialmente rientrante tra quelli ad alto rischio può essere introdotto o utilizzato nell'organizzazione dell'Ente senza che siano stati preventivamente individuati gli obblighi normativi applicabili e definite le relative misure organizzative, tecniche e procedurali.

Art. 12 – Sistemi di IA rivolti ai cittadini

1. Qualora il Comune utilizzi sistemi di IA con i quali cittadini, utenti o imprese possano interagire direttamente, l'Ente assicura, nei casi previsti dalla normativa applicabile, un'informazione chiara circa la natura automatizzata dell'interazione.

2. I sistemi destinati a fornire informazioni o assistenza agli utenti devono essere progettati e configurati in modo da:

- a) evitare di presentare il sistema come un operatore umano;
- b) rendere riconoscibile la natura automatizzata dell'interazione nei casi previsti dalla normativa;
- c) consentire, quando necessario, il passaggio a un operatore umano;
- d) fornire informazioni coerenti con le competenze istituzionali dell'Ente;
- e) evitare la raccolta di dati eccedenti rispetto alle finalità del servizio;
- f) garantire adeguati livelli di sicurezza;
- g) evitare che le risposte generate automaticamente siano presentate come provvedimenti, decisioni, pareri ufficiali o comunicazioni aventi valore amministrativo, salvo che siano state previamente validate e adottate secondo le procedure dell'Ente.

3. L'utilizzo di un chatbot o di altro sistema automatizzato non esonera l'Amministrazione dagli obblighi di trasparenza, accessibilità, protezione dei dati, sicurezza e corretta informazione previsti dalla normativa vigente.

4. Quando la natura del servizio lo richieda, devono essere definite modalità per consentire all'utente di richiedere l'intervento di un operatore umano o di ottenere informazioni sulle modalità di trattamento della richiesta.

Art. 13 – Contenuti generati o modificati mediante IA

1. L'utilizzo dell'IA per la produzione di testi, immagini, audio, video o altri contenuti destinati alla comunicazione istituzionale deve essere sottoposto a verifica e validazione umana.
2. Nei casi in cui la normativa europea o nazionale imponga specifici obblighi di informazione, marcatura o identificazione dei contenuti generati o manipolati mediante IA, l'Ente provvede al relativo adempimento.
3. L'Ente può prevedere, attraverso proprie disposizioni organizzative, ulteriori forme di trasparenza sull'utilizzo dell'IA nella comunicazione istituzionale, anche quando non espressamente imposte dalla normativa.
4. La verifica umana deve assicurare, in particolare, che il contenuto:
 - a) sia corretto e coerente con le informazioni ufficiali dell'Ente;
 - b) non induca in errore;
 - c) non attribuisca all'Amministrazione contenuti non approvati;
 - d) rispetti i diritti d'autore e gli altri diritti di proprietà intellettuale;
 - e) non contenga informazioni riservate o dati personali trattati illecitamente;
 - f) non utilizzi, senza adeguata verifica, contenuti provenienti da fonti la cui utilizzazione sia soggetta a restrizioni.
5. La verifica deve riguardare, ove pertinente, anche la legittimità dell'utilizzo dei contenuti forniti come input al sistema e delle modalità di riutilizzo, trasformazione o pubblicazione dell'output.

Art. 14 – Acquisizione di sistemi e servizi di IA

1. L'acquisizione di sistemi o servizi basati sull'IA deve essere preceduta da una valutazione della loro adeguatezza rispetto alle finalità dell'Ente e ai rischi connessi al loro utilizzo.
2. Nei procedimenti di acquisizione devono essere valutati, per quanto pertinenti:
 - a) finalità e caratteristiche del sistema;
 - b) categoria e livello di rischio;
 - c) trattamento e localizzazione dei dati;
 - d) condizioni di conservazione e cancellazione dei dati;
 - e) eventuale riutilizzo dei dati da parte del fornitore;
 - f) sicurezza informatica;
 - g) interoperabilità e portabilità;
 - h) possibilità di audit e controllo;
 - i) tracciabilità delle operazioni;
 - j) modalità di aggiornamento del sistema;
 - k) responsabilità del fornitore e dell'Amministrazione;
 - l) condizioni di cessazione del servizio;
 - m) conformità alla normativa europea e nazionale applicabile.
3. Per le acquisizioni di sistemi di IA devono essere tenute in considerazione, per quanto applicabili, le indicazioni e le Linee Guida AgID vigenti al momento dell'acquisizione.
4. I capitolati, gli atti di gara e i contratti devono contenere, ove pertinenti, clausole idonee a garantire il rispetto degli obblighi in materia di protezione dei dati, sicurezza, riservatezza, trasparenza, continuità operativa, audit, gestione degli incidenti, proprietà intellettuale e conformità normativa.

5. Nei contratti relativi a sistemi o servizi di IA devono essere individuate, ove pertinenti, le responsabilità del fornitore e dell'Amministrazione lungo il ciclo di vita del sistema, comprese le responsabilità relative agli aggiornamenti, alle modifiche sostanziali, alla gestione delle vulnerabilità e alla cessazione del servizio.

6. La presenza di funzionalità di IA all'interno di applicativi, piattaforme, servizi cloud o altri strumenti acquisiti dall'Ente deve essere dichiarata dal fornitore e sottoposta alle verifiche previste dalle presenti Linee Guida quando tali funzionalità siano suscettibili di incidere sulla sicurezza, sulla protezione dei dati personali, sui procedimenti amministrativi o sui diritti delle persone.

Art. 15 – Censimento dei sistemi di IA

1. Il Comune istituisce il **Registro interno dei sistemi e dei casi d'uso di Intelligenza Artificiale**, quale strumento organizzativo per il censimento, il monitoraggio e la governance degli utilizzi dell'IA nell'Ente.

2. Il Registro deve comprendere, almeno:

- a) denominazione del sistema o servizio;
- b) fornitore;
- c) struttura utilizzatrice;
- d) finalità;
- e) tipologia di IA utilizzata;
- f) categorie di dati trattati;
- g) presenza di dati personali;
- h) eventuale utilizzo di dati riservati;
- i) modalità di acquisizione;
- j) livello di autonomia;
- k) eventuale interazione con cittadini;
- l) valutazione preliminare del rischio;
- m) eventuale classificazione ai sensi dell'AI Act;
- n) misure di controllo umano;
- o) referente interno;
- p) data dell'ultima verifica.

3. Il censimento è aggiornato periodicamente e comunque in occasione dell'introduzione di nuovi sistemi o di modifiche sostanziali alle modalità di utilizzo di sistemi esistenti.

4. Il Registro è tenuto secondo modalità definite dal RTD, nel rispetto delle competenze delle strutture interessate e della normativa in materia di protezione dei dati personali, sicurezza delle informazioni e gestione documentale.

5. Per ciascun sistema o caso d'uso sono conservate, ove applicabili, la scheda di valutazione preliminare, la documentazione relativa alle valutazioni effettuate, gli atti di acquisizione, le informazioni relative al fornitore, le misure di controllo adottate e le evidenze delle verifiche periodiche.

6. Il Registro costituisce strumento organizzativo interno dell'Ente e la sua eventuale pubblicazione, totale o parziale, è effettuata esclusivamente nei casi e secondo le modalità previste dalla normativa vigente.

Art. 16 – Governance dell'Intelligenza Artificiale

1. La governance dell'IA nell'Ente è assicurata attraverso il coordinamento delle competenze previste dall'ordinamento comunale e dalle presenti Linee Guida, nel rispetto delle attribuzioni dei singoli soggetti e strutture.
2. Il **Responsabile per la Transizione al Digitale (RTD)**, nell'ambito delle proprie competenze, svolge funzioni di coordinamento e impulso per gli aspetti di innovazione digitale, censimento dei sistemi e dei casi d'uso, governance tecnologica, diffusione delle competenze digitali e raccordo con le indicazioni nazionali ed europee in materia di IA.
3. Il RTD non assume, per effetto delle presenti Linee Guida, le responsabilità gestionali, amministrative o decisionali proprie dei dirigenti, dei responsabili dei procedimenti o delle altre strutture competenti.
4. Il **Responsabile della Protezione dei Dati (DPO)** è coinvolto nei casi in cui l'utilizzo dell'IA comporti questioni rilevanti in materia di protezione dei dati personali, secondo le competenze attribuitegli dal Regolamento (UE) 2016/679.
5. Il coinvolgimento del DPO non comporta l'attribuzione allo stesso di responsabilità operative o decisionali in ordine alla progettazione, acquisizione, configurazione o utilizzo dei sistemi di IA, restando ferme le funzioni e i compiti previsti dall'articolo 39 del Regolamento (UE) 2016/679.
6. I dirigenti e i responsabili delle strutture organizzative:
 - a) individuano gli utilizzi dell'IA nell'ambito delle rispettive strutture;
 - b) assicurano il rispetto delle presenti Linee Guida;
 - c) assicurano che le valutazioni preliminari previste siano effettuate prima dell'avvio dei casi d'uso che lo richiedono;
 - d) promuovono la formazione del personale interessato;
 - e) assicurano la corretta registrazione e l'aggiornamento delle informazioni relative ai sistemi utilizzati;
 - f) segnalano al RTD e alle altre strutture competenti eventuali criticità, incidenti o utilizzi potenzialmente ad alto rischio.
7. Restano ferme le competenze del responsabile della sicurezza informatica, del responsabile della gestione documentale, del responsabile della conservazione, del DPO e delle altre figure previste dall'organizzazione dell'Ente.
8. La responsabilità della decisione di utilizzare uno specifico sistema di IA nell'ambito di un'attività o procedimento resta in capo alla struttura competente secondo l'ordinamento dell'Ente.

Art. 17 – Alfabetizzazione e formazione del personale

1. Il Comune assicura un adeguato livello di **AI Literacy** per il personale che utilizza sistemi di IA nell'esercizio delle proprie funzioni, in attuazione dell'articolo 4 del Regolamento (UE) 2024/1689.
2. La formazione è proporzionata:
 - a) al ruolo ricoperto;
 - b) alle competenze possedute;
 - c) al livello di autonomia del sistema utilizzato;
 - d) alla natura delle attività svolte;
 - e) ai rischi connessi al trattamento dei dati e all'impatto sui cittadini;
 - f) all'eventuale utilizzo di sistemi ad alto rischio.

3. La formazione di base deve comprendere almeno:

- a) principi e funzionamento generale dell'IA;
- b) opportunità e limiti dell'IA generativa;
- c) errori e allucinazioni;
- d) verifica delle informazioni;
- e) protezione dei dati personali;
- f) riservatezza e segreto d'ufficio;
- g) sicurezza informatica;
- h) responsabilità dell'operatore;
- i) principali obblighi dell'AI Act;
- j) regole interne dell'Ente.

4. Per dirigenti, RTD, personale informatico, DPO e personale operante in settori maggiormente esposti ai rischi dell'IA devono essere previsti, ove necessario, percorsi specialistici.

5. Le attività formative sono raccordate con la programmazione della formazione del personale e con il PIAO.

Art. 18 – Utilizzi vietati

1. È vietato utilizzare sistemi di IA in violazione della normativa vigente, del Regolamento (UE) 2024/1689, delle presenti Linee Guida o delle disposizioni organizzative e di sicurezza dell'Ente.

2. È in particolare vietato:

- a) utilizzare pratiche di IA vietate dal Regolamento (UE) 2024/1689 o da altra normativa applicabile;
- b) utilizzare sistemi di IA per finalità diverse da quelle autorizzate o dichiarate;
- c) inserire dati personali, categorie particolari di dati personali, dati giudiziari o informazioni riservate in sistemi non autorizzati o non preventivamente valutati;
- d) utilizzare l'output dell'IA come unica fonte per assumere decisioni amministrative rilevanti;
- e) presentare come verificata un'informazione generata dall'IA che non sia stata effettivamente verificata;
- f) utilizzare l'IA per eludere procedure, controlli o responsabilità previste dall'ordinamento;
- g) utilizzare sistemi di IA in modo discriminatorio o lesivo dei diritti delle persone;
- h) utilizzare account personali o strumenti non autorizzati per trattare informazioni dell'Ente quando tale utilizzo non sia compatibile con le disposizioni di sicurezza e protezione dei dati;
- i) utilizzare sistemi di IA per generare contenuti fraudolenti, ingannevoli o contrari alla legge.

3. La mera riconducibilità di un sistema alle categorie di sistemi di IA ad alto rischio non determina, di per sé, il divieto di utilizzo. In tali casi devono essere previamente individuati e adempiuti gli obblighi previsti dal Regolamento (UE) 2024/1689 e dalla normativa applicabile.

4. Restano ferme le ulteriori pratiche vietate dal Regolamento (UE) 2024/1689 e dalla normativa europea, nazionale e regionale vigente.

Art. 19 – Segnalazione di incidenti e criticità

1. Il personale che rilevi, in relazione all'utilizzo di un sistema di IA:

- a) divulgazione o perdita di dati;

- b) accesso non autorizzato;
- c) comportamento anomalo del sistema;
- d) output manifestamente errati con potenziale impatto amministrativo;
- e) discriminazioni o risultati potenzialmente lesivi dei diritti;
- f) violazioni delle presenti Linee Guida;
- g) altri eventi suscettibili di compromettere la sicurezza o la correttezza dell'attività amministrativa.

deve procedere alla tempestiva segnalazione secondo le procedure interne dell'Ente.

2. Qualora l'evento riguardi dati personali, la segnalazione deve essere effettuata anche secondo le procedure interne relative agli incidenti di sicurezza e alle violazioni dei dati personali (data breach).
3. Qualora l'evento riguardi un sistema di IA ad alto rischio, devono essere applicate, ove pertinenti, anche le procedure di monitoraggio, segnalazione e gestione degli incidenti previste dal Regolamento (UE) 2024/1689 e dalle istruzioni del fornitore.
4. In presenza di un evento che possa comportare un rischio per i diritti delle persone, per la sicurezza delle informazioni o per la continuità dell'attività amministrativa, la struttura competente valuta, secondo le procedure dell'Ente, la necessità di sospendere temporaneamente l'utilizzo del sistema.
5. Le segnalazioni sono utilizzate anche per migliorare progressivamente le misure organizzative, tecniche e formative dell'Ente.

Art. 20 – Monitoraggio e aggiornamento

1. Il Comune monitora periodicamente l'evoluzione normativa, tecnologica e organizzativa in materia di IA e verifica l'adeguatezza delle presenti Linee Guida rispetto ai sistemi e ai casi d'uso presenti nell'Ente.
2. Le presenti Linee Guida sono aggiornate quando:
 - a) intervengano modifiche della normativa europea o nazionale;
 - b) siano emanati provvedimenti o indicazioni vincolanti delle autorità competenti;
 - c) siano adottate pertinenti Linee Guida AgID;
 - d) siano introdotti nell'Ente nuovi sistemi o modalità di utilizzo dell'IA;
 - e) emergano criticità dall'attività di monitoraggio;
 - f) intervengano modifiche significative nell'organizzazione dell'Ente o nelle responsabilità delle strutture coinvolte.
3. Il monitoraggio tiene conto anche dell'evoluzione degli obblighi applicabili ai sistemi ad alto rischio, delle relative scadenze e degli eventuali atti di esecuzione, orientamenti e ulteriori disposizioni applicabili.
4. In caso di modifiche normative che rendano incompatibile una disposizione delle presenti Linee Guida con una norma europea o nazionale direttamente applicabile, prevale la disposizione normativa sopravvenuta, fermo restando l'obbligo di procedere al successivo aggiornamento formale delle Linee Guida.

Art. 21 – Rapporti con le altre discipline interne

1. Le presenti Linee Guida integrano e non sostituiscono:
 - a) il regolamento comunale sull'ordinamento degli uffici e dei servizi;

- b) le disposizioni in materia di protezione dei dati personali;
- c) le disposizioni in materia di sicurezza informatica;
- d) le policy sull'utilizzo delle apparecchiature e delle risorse informatiche;
- e) le disposizioni in materia di gestione documentale;
- f) il codice di comportamento dei dipendenti pubblici;
- g) le disposizioni in materia di trasparenza e accesso;
- h) le procedure relative agli affidamenti e ai contratti pubblici;
- i) ogni altra disposizione applicabile all'attività amministrativa.

2. In caso di contrasto, prevalgono le disposizioni normative e regolamentari di rango superiore.

Art. 22 – Entrata in vigore

Le presenti Linee Guida entrano in vigore dalla data di esecutività della deliberazione della Giunta Comunale che le approva.

APPENDICE OPERATIVA

Classificazione interna degli utilizzi dell'IA

Ai fini dell'applicazione delle presenti Linee Guida, gli utilizzi dei sistemi di IA sono ricondotti, in via organizzativa interna e senza sostituire le classificazioni previste dalla normativa europea e nazionale, ai seguenti quattro livelli di controllo.

☐ LIVELLO 1 – Utilizzo ordinario

Rientrano, a titolo esemplificativo:

- correzione grammaticale, ortografica e stilistica di testi;
- traduzione di testi privi di dati personali o informazioni riservate;
- elaborazione di schemi e strutture di documenti;
- sintesi di informazioni pubblicamente disponibili;
- brainstorming;
- preparazione di materiali formativi;
- supporto alla redazione di comunicazioni non contenenti informazioni riservate;
- elaborazione di checklist, prospetti e materiali di lavoro.

Condizione: l'output deve essere verificato dall'operatore prima dell'utilizzo nell'attività dell'Ente.

☐ LIVELLO 2 – Utilizzo con cautele

Rientrano, a titolo esemplificativo:

- redazione assistita di bozze di atti amministrativi;
- elaborazione o sintesi di documentazione interna non contenente dati o informazioni soggette a particolari vincoli;
- utilizzo di funzionalità IA integrate in software gestionali o applicativi dell'Ente;
- chatbot rivolti ai cittadini per attività informative;
- elaborazione di documenti destinati alla pubblicazione;
- analisi preliminare di dati previamente anonimizzati o adeguatamente protetti;

- utilizzo dell'IA nell'ambito delle procedure di acquisizione di beni e servizi.

Condizioni: verifica dell'output, rispetto delle misure di sicurezza e protezione dei dati e applicazione delle ulteriori cautele previste dalle presenti Linee Guida.

☐ **LIVELLO 3 – Utilizzo soggetto a preventiva valutazione**

Rientrano, a titolo esemplificativo:

- sistemi che trattano dati personali non pubblicamente disponibili;
- sistemi che trattano categorie particolari di dati personali o dati relativi a condanne penali e reati;
- sistemi che trattano informazioni riservate;
- sistemi di profilazione;
- sistemi che interagiscono direttamente con cittadini nell'ambito di servizi pubblici;
- sistemi integrati in procedimenti amministrativi;
- sistemi che possono incidere significativamente sui diritti o sugli interessi delle persone;
- sistemi utilizzati per la selezione, valutazione o gestione del personale;
- sistemi utilizzati nell'ambito delle attività della Polizia Locale;
- sistemi biometrici;
- sistemi che possono rientrare nelle categorie di sistemi ad alto rischio;
- sistemi acquisiti o sviluppati dall'Ente che presentino specifici rischi giuridici, organizzativi, tecnologici o di sicurezza.

Condizione: preventiva valutazione documentata del caso d'uso e, ove necessario, coinvolgimento del RTD, DPO, responsabile della sicurezza informatica e delle altre strutture competenti.

☐ **LIVELLO 4 – Utilizzo vietato**

Rientrano in questo livello esclusivamente gli utilizzi vietati dalla normativa europea o nazionale o dalle presenti Linee Guida, tra cui:

- le pratiche di IA vietate dal Regolamento (UE) 2024/1689;
- utilizzi contrari alla normativa vigente;

- inserimento non autorizzato di dati personali o informazioni riservate in sistemi IA;
- utilizzi fraudolenti o ingannevoli;
- utilizzi finalizzati ad eludere controlli, procedure o responsabilità;
- utilizzi discriminatori o lesivi dei diritti delle persone;
- decisioni completamente automatizzate quando non consentite dalla normativa applicabile;
- utilizzi di sistemi per i quali siano obbligatorie valutazioni o autorizzazioni preventive che non siano state effettuate.

Condizione: l'utilizzo non è consentito.

Principio di distinzione

La classificazione interna di cui alla presente Appendice ha esclusiva funzione organizzativa e **non sostituisce la classificazione giuridica prevista dal Regolamento (UE) 2024/1689.**

In particolare, la riconducibilità di un sistema alla categoria dei sistemi di IA ad alto rischio **non comporta automaticamente il divieto di utilizzo**, ma determina l'applicazione degli specifici obblighi previsti dalla normativa vigente.

PRINCIPIO FINALE

“L'IA supporta l'azione amministrativa; non sostituisce la responsabilità umana.”

Ogni utilizzo dell'intelligenza artificiale nell'Amministrazione deve essere orientato all'interesse pubblico, rispettare la dignità e i diritti delle persone e mantenere un livello di controllo umano adeguato alla natura e ai rischi dell'attività.