

POLITICA PER L'USO RESPONSABILE DELL'INTELLIGENZA ARTIFICIALE

ai sensi del Regolamento (UE) 2024/1689, della Legge 23 settembre 2025, n. 132, del
Regolamento (UE) 2016/679 e della normativa applicabile

1. PREMESSE E RIFERIMENTI

La presente Politica disciplina l'adozione, l'acquisizione, lo sviluppo, la sperimentazione e l'utilizzo di sistemi di Intelligenza Artificiale, di seguito "IA", nell'ambito delle attività istituzionali del Comune di Noicattaro.

La Politica è adottata nel rispetto del Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, che stabilisce regole armonizzate sull'intelligenza artificiale ("AI Act"), della Legge 23 settembre 2025, n. 132, recante disposizioni e deleghe al Governo in materia di intelligenza artificiale, del Regolamento (UE) 2016/679 ("GDPR"), del d.lgs. 30 giugno 2003, n. 196, del d.lgs. 7 marzo 2005, n. 82 ("Codice dell'Amministrazione Digitale"), del d.lgs. 31 marzo 2023, n. 36, della normativa nazionale ed europea in materia di cybersicurezza, nonché delle ulteriori disposizioni normative, regolamentari e contrattuali applicabili.

L'Ente tiene altresì conto del Piano Triennale per l'Informatica nella Pubblica Amministrazione, della Strategia italiana per l'intelligenza artificiale e delle Linee guida, raccomandazioni, strumenti operativi e documenti emanati o posti in consultazione da AgID e dalle altre autorità competenti, secondo il rispettivo stato di adozione ed efficacia.

La presente Politica costituisce parte integrante del sistema di governance digitale, di protezione dei dati personali, di sicurezza informatica, di gestione documentale, di gestione del rischio e di prevenzione della corruzione dell'Ente.

L'adozione dell'IA deve perseguire finalità istituzionali determinate e assicurare un utilizzo consapevole della tecnologia, preservando la centralità della persona, il buon andamento, l'imparzialità e la responsabilità dell'azione amministrativa.

2. DEFINIZIONI

Ai fini della presente Politica si intende per:

Ente: il Comune di Noicattaro.

Sistema di IA: un sistema basato su macchina progettato per funzionare con livelli variabili di autonomia e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input ricevuto come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali.

IA generativa: sistema di IA idoneo a generare nuovi contenuti, tra cui testi, immagini, audio, video, codice informatico, elaborazioni, sintesi o altri output.

Modello di IA per finalità generali – GPAI: modello di IA caratterizzato da una generalità significativa e capace di svolgere in modo competente un'ampia gamma di compiti distinti, secondo quanto previsto dall'AI Act.

Provider: soggetto che sviluppa un sistema o modello di IA o lo fa sviluppare e lo immette sul mercato o lo mette in servizio con il proprio nome o marchio.

Deployer: persona fisica o giuridica, autorità pubblica, agenzia o altro organismo che utilizza un sistema di IA sotto la propria autorità, salvo il caso in cui il sistema sia utilizzato nel corso di un'attività personale non professionale. Nell'utilizzo istituzionale dei sistemi di IA il Comune può assumere, di regola, il ruolo di deployer, ferme restando le verifiche da effettuare sul ruolo effettivamente assunto in ciascun progetto.

Sistema di IA ad alto rischio: sistema rientrante nelle condizioni previste dall'articolo 6 e dagli Allegati pertinenti del Regolamento (UE) 2024/1689, tenendo conto delle eventuali condizioni ed eccezioni previste dal medesimo Regolamento.

FRIA – Fundamental Rights Impact Assessment: valutazione d'impatto sui diritti fondamentali prevista dall'articolo 27 del Regolamento (UE) 2024/1689 nei casi in cui essa sia obbligatoria.

DPIA – Data Protection Impact Assessment: valutazione d'impatto sulla protezione dei dati personali prevista dall'articolo 35 GDPR.

Human oversight: insieme delle misure di supervisione umana destinate a prevenire o minimizzare i rischi derivanti dall'utilizzo di un sistema IA e a garantire che la persona competente possa comprendere, controllare e, quando necessario, non utilizzare, interrompere o disattivare il sistema o non recepirne l'output.

Referente IA: soggetto eventualmente individuato dall'Ente con funzioni di coordinamento operativo della governance dei sistemi di IA, ferme restando le competenze attribuite dalla legge agli altri soggetti.

Registro IA: inventario dei sistemi di IA proposti, sperimentati, autorizzati, in uso o dismessi dall'Ente.

Utilizzo autorizzato: utilizzo di un sistema IA sottoposto al processo di valutazione previsto dalla presente Politica e formalmente ammesso dall'Ente per specifici casi d'uso.

3. FINALITÀ E AMBITO DI APPLICAZIONE

La presente Politica definisce le regole, le responsabilità e il processo di governance relativi all'intero ciclo di vita dei sistemi di IA utilizzati dall'Ente.

Essa si applica alla selezione, acquisizione, progettazione, sviluppo, sperimentazione, configurazione, utilizzo operativo, monitoraggio, manutenzione, modifica, aggiornamento e dismissione dei sistemi di IA.

La Politica si applica a dipendenti, dirigenti, collaboratori, consulenti, tirocinanti e, per quanto previsto dai relativi atti contrattuali, fornitori, responsabili del trattamento, sub-responsabili e partner tecnologici.

Le disposizioni si applicano anche quando strumenti di IA vengono utilizzati mediante dispositivi personali per svolgere attività lavorative o istituzionali.

È vietato utilizzare strumenti, account o servizi di IA personali o non autorizzati per trattare informazioni, documenti o dati dell'Ente.

4. PRINCIPI GENERALI

L'adozione e l'utilizzo dell'IA da parte dell'Ente sono ispirati ai principi di legalità, necessità, proporzionalità, responsabilità, trasparenza, sicurezza, accuratezza, affidabilità, accessibilità, non discriminazione, sostenibilità, protezione dei dati personali e rispetto dei diritti fondamentali.

L'Ente assicura in particolare:

Centralità della persona. I sistemi IA devono essere utilizzati nel rispetto della dignità, dell'autonomia e dei diritti e delle libertà fondamentali delle persone.

Responsabilità umana. L'IA costituisce, di regola, uno strumento di supporto e non determina un trasferimento della responsabilità amministrativa o professionale dal soggetto competente al sistema tecnologico o al relativo fornitore.

Supervisione umana. Gli output rilevanti ai fini dell'attività amministrativa devono essere sottoposti a controllo umano adeguato al rischio e al contesto di utilizzo.

Non discriminazione. Devono essere prevenuti, individuati e gestiti bias, distorsioni e discriminazioni dirette o indirette.

Trasparenza e conoscibilità. L'utilizzo dell'IA deve essere documentabile e, quando previsto dalla normativa o necessario per assicurare correttezza e trasparenza nei confronti degli interessati, reso conoscibile.

Qualità dei dati. I dati utilizzati devono essere pertinenti, adeguati, aggiornati e proporzionati rispetto alle finalità perseguite.

Protezione dei dati personali. Qualsiasi trattamento di dati personali mediante sistemi IA deve rispettare il GDPR e la normativa nazionale applicabile.

Sicurezza. I sistemi devono essere sottoposti a misure tecniche e organizzative proporzionate ai relativi rischi.

Accountability. Le valutazioni, le autorizzazioni, i controlli e le decisioni significative riguardanti l'utilizzo dell'IA devono essere documentati.

5. CLASSIFICAZIONE DEI SISTEMI E DEGLI UTILIZZI DI IA

Prima dell'autorizzazione di qualsiasi nuovo sistema o caso d'uso, l'Ente effettua una valutazione preliminare volta a determinare la disciplina applicabile.

La classificazione considera almeno:

- a) l'eventuale riconducibilità alle pratiche vietate dall'articolo 5 AI Act;
- b) l'eventuale qualificazione del sistema come sistema ad alto rischio ai sensi dell'articolo 6 e degli Allegati pertinenti dell'AI Act;
- c) l'applicabilità degli obblighi di trasparenza previsti dall'AI Act, incluso l'articolo 50;
- d) l'eventuale impiego di modelli di IA per finalità generali;
- e) la presenza di dati personali, categorie particolari di dati personali o dati relativi a condanne penali e reati;
- f) l'incidenza del sistema su persone fisiche, lavoratori, cittadini, imprese o procedimenti amministrativi;
- g) l'eventuale necessità di una DPIA o di una FRIA;
- h) i rischi per sicurezza, disponibilità, autenticità, integrità e riservatezza delle informazioni;
- i) il livello di autonomia del sistema e l'effettiva capacità di supervisione umana.

L'Ente può adottare una classificazione interna ulteriore per graduare i controlli organizzativi, purché essa non sostituisca le categorie e gli obblighi previsti dall'AI Act.

6. PRATICHE DI IA VIETATE

È vietata l'adozione o l'utilizzo da parte dell'Ente delle pratiche di IA vietate dall'articolo 5 del Regolamento (UE) 2024/1689, nel testo vigente.

A titolo esemplificativo e non esaustivo, sono vietati gli utilizzi che:

- a) impiegano tecniche subliminali, manipolative o ingannevoli nelle condizioni vietate dalla normativa;
- b) sfruttano vulnerabilità connesse, tra l'altro, all'età, alla disabilità o a specifiche condizioni personali o sociali al fine di alterare significativamente il comportamento delle persone provocando o potendo provocare un danno significativo;

c) realizzano forme di social scoring vietate;

d) ricadono nelle ipotesi vietate concernenti determinate forme di categorizzazione biometrica, riconoscimento delle emozioni, creazione o ampliamento di banche dati per il riconoscimento facciale, valutazione del rischio di commissione di reati o identificazione biometrica remota, salvo le specifiche eccezioni previste dalla normativa.

In caso di dubbio sulla riconducibilità di un progetto alle pratiche vietate, l'attivazione del sistema è sospesa fino alla conclusione della valutazione.

7. GOVERNANCE E RESPONSABILITÀ

La governance dell'IA si fonda sulla separazione dei ruoli, sull'individuazione delle responsabilità e sulla collaborazione interdisciplinare.

Il **Responsabile della Transizione Digitale – RTD** coordina, per quanto di competenza, l'attuazione della strategia dell'Ente in materia di IA, assicurando la coerenza con i processi di trasformazione digitale e con il sistema informativo dell'Amministrazione.

I **dirigenti e responsabili delle strutture** sono responsabili delle finalità istituzionali perseguite, della necessità del sistema, della correttezza del caso d'uso e dell'effettivo rispetto delle prescrizioni della presente Politica nell'ambito delle attività di propria competenza.

Il **Responsabile ICT/Cybersecurity**, o la struttura competente, valuta l'architettura tecnica, la sicurezza del sistema, le integrazioni, le vulnerabilità, il logging, la continuità operativa, le modalità di accesso e gli ulteriori profili tecnici.

Il **RPD/DPO** è tempestivamente consultato per gli aspetti che riguardano la protezione dei dati personali secondo gli articoli 38 e 39 GDPR e fornisce consulenza in relazione alla necessità e allo svolgimento della DPIA. Il RPD/DPO opera in autonomia e indipendenza e non assume responsabilità decisionali o gestionali in merito alla scelta, autorizzazione o messa in esercizio dei sistemi di IA.

Il **Responsabile della prevenzione della corruzione e della trasparenza – RPCT**, ove pertinente rispetto alle caratteristiche del sistema, può essere coinvolto nella valutazione dei rischi di opacità, alterazione dei procedimenti, conflitti di interessi, trasparenza e integrità amministrativa.

L'Ente può nominare un **Referente IA**, con funzioni di coordinamento tecnico-organizzativo, tenuta del Registro IA, supporto alle strutture proponenti, raccolta della documentazione, monitoraggio e coordinamento delle iniziative di formazione.

La nomina del Referente IA non comporta trasferimento delle responsabilità attribuite dalla normativa ai dirigenti, al titolare del trattamento, al RTD, al RPD/DPO o agli altri soggetti competenti.

L'Ente può istituire un **Gruppo interdisciplinare IA**, composto, in funzione del caso concreto, da RTD, ICT/Cybersecurity, Referente IA, ufficio legale, procurement, responsabile della struttura interessata, RPD/DPO quale funzione consultiva per gli aspetti privacy, RPCT e ulteriori professionalità necessarie.

8. PROCESSO DI PROPOSTA, VALUTAZIONE E AUTORIZZAZIONE

Nessun sistema IA può essere impiegato per finalità istituzionali senza essere stato preventivamente valutato e, salvo gli usi espressamente ammessi dalla presente Politica o da specifici atti interni, autorizzato dall'Ente.

La struttura interessata presenta una richiesta descrivendo almeno finalità, processo interessato, utenti, dati utilizzati, output attesi, fornitore, modalità di accesso, eventuali integrazioni e benefici attesi.

La valutazione preliminare comprende, in misura proporzionata al rischio:

- a) verifica della natura IA del sistema;
- b) individuazione dei ruoli previsti dall'AI Act;
- c) verifica delle pratiche vietate;
- d) classificazione del rischio;
- e) verifica dell'eventuale applicabilità dell'articolo 50 AI Act;
- f) verifica dei trattamenti di dati personali;
- g) screening DPIA;
- h) screening FRIA;
- i) verifica di sicurezza e cybersecurity;
- j) valutazione del fornitore;
- k) verifica degli aspetti contrattuali e di procurement;
- l) valutazione della supervisione umana;
- m) valutazione dell'accuratezza e dell'affidabilità attese;
- n) individuazione delle misure di monitoraggio;
- o) determinazione degli obblighi di trasparenza.

Il sistema può essere messo in esercizio solo a seguito dell'esito favorevole del processo e dell'iscrizione nel Registro IA.

L'autorizzazione indica il caso d'uso consentito. Qualsiasi impiego sostanzialmente diverso deve essere sottoposto a nuova valutazione.

9. REGISTRO DEI SISTEMI DI IA

L'Ente istituisce e mantiene aggiornato un Registro dei sistemi di IA.

Il Registro contiene, almeno:

denominazione e versione del sistema; fornitore; struttura utilizzatrice; referente interno; finalità; caso d'uso; ruolo dell'Ente ai sensi dell'AI Act; classificazione; categorie di utenti; categorie di persone interessate; presenza e tipologia di dati personali; eventuale responsabile del trattamento; esito dello screening DPIA e FRIA; data dell'eventuale DPIA o FRIA; misure di human oversight; modalità di logging; data di autorizzazione; data dell'ultimo riesame; incidenti rilevanti; modifiche sostanziali; data e modalità di dismissione.

Il Registro costituisce strumento interno di accountability e può alimentare, nei casi previsti dalla legge, ulteriori registrazioni, comunicazioni o forme di pubblicità obbligatorie.

10. UTILIZZO DELL'IA GENERATIVA

Gli strumenti di IA generativa possono essere utilizzati esclusivamente nei limiti delle finalità istituzionali e secondo le autorizzazioni dell'Ente.

Il personale utilizza esclusivamente strumenti presenti nell'elenco dei servizi autorizzati, attraverso le modalità e gli account individuati dall'Amministrazione.

È vietato inserire in sistemi IA non autorizzati:

dati personali; categorie particolari di dati personali; dati relativi a condanne penali e reati; dati coperti da segreto; documenti riservati; credenziali; password; chiavi crittografiche; token; configurazioni di sicurezza; vulnerabilità non pubbliche; informazioni confidenziali; documenti non destinati alla divulgazione; informazioni relative a procedimenti riservati; dati o contenuti di terzi per i quali non ricorrano le condizioni di liceità dell'utilizzo.

L'utilizzo di dati personali all'interno di un sistema IA autorizzato non è di per sé vietato, ma deve essere previamente valutato e risultare necessario, proporzionato e conforme alla normativa applicabile.

Devono essere utilizzati, ove possibile, dati anonimi, aggregati, sintetici o previamente minimizzati.

L'utente deve considerare il prompt, gli allegati e gli altri contenuti comunicati al sistema come informazioni potenzialmente trattate dal fornitore secondo le condizioni tecniche e contrattuali del servizio.

Gli output dell'IA generativa non costituiscono fonti attendibili per il solo fatto di essere prodotti dal sistema.

Prima dell'utilizzo di un output il dipendente deve verificarne, in funzione della rilevanza del caso:

accuratezza; completezza; coerenza; attendibilità delle fonti; aggiornamento normativo; eventuali citazioni inesistenti; errori fattuali; contenuti discriminatori; violazioni di diritti di proprietà intellettuale; rischi di divulgazione di informazioni riservate.

È vietato presentare come verificato un contenuto prodotto dall'IA che non sia stato sottoposto ad adeguato controllo umano.

La generazione automatica di codice destinato a sistemi dell'Ente richiede verifiche di sicurezza, qualità, dipendenze software, licenze e vulnerabilità prima della messa in produzione.

L'utilizzo di immagini, audio o video sintetici deve rispettare gli obblighi di trasparenza previsti dalla normativa e non deve essere idoneo a ingannare gli utenti circa l'origine o l'autenticità del contenuto.

11. IA NELL'ATTIVITÀ E NEI PROCEDIMENTI AMMINISTRATIVI

L'utilizzo dell'IA nell'attività amministrativa ha funzione strumentale e di supporto.

Restano impregiudicati l'autonomia, il potere valutativo e la responsabilità del responsabile del procedimento, del dirigente e del soggetto competente all'adozione dell'atto o provvedimento.

Gli output generati da sistemi IA non possono essere recepiti in maniera automatica o acritica quando incidono sull'esercizio di funzioni amministrative.

Il soggetto competente deve poter comprendere la funzione svolta dal sistema, valutare la pertinenza dell'output e discostarsene.

Quando l'IA contribuisce in misura significativa all'istruttoria o alla predisposizione di un atto, l'Ente assicura un livello di tracciabilità proporzionato al relativo impatto, ferme restando le disposizioni applicabili alla motivazione del provvedimento, all'accesso agli atti, alla trasparenza e alla protezione dei dati personali.

È vietato affidare a un sistema IA la decisione finale nei casi in cui ciò contrasti con la normativa applicabile o impedisca un'effettiva valutazione umana.

Resta ferma l'applicazione dell'articolo 22 GDPR nei casi di decisioni basate unicamente sul trattamento automatizzato che producano effetti giuridici o incidano in modo analogo significativamente sulla persona.

12. SISTEMI AD ALTO RISCHIO E SUPERVISIONE UMANA

Prima dell'utilizzo di un sistema classificato ad alto rischio, l'Ente verifica l'adempimento degli obblighi applicabili al deployer e acquisisce dal provider la documentazione necessaria.

Devono essere individuate persone fisiche incaricate della supervisione umana, dotate di competenza, autorità e formazione adeguate.

La supervisione deve consentire, in funzione del sistema:

di comprenderne capacità e limiti; di riconoscere anomalie e malfunzionamenti; di evitare un affidamento automatico sull'output; di interpretare correttamente l'output; di decidere di non utilizzare il sistema o il relativo risultato; di interrompere l'operatività quando necessario.

Per i sistemi ad alto rischio devono essere assicurate le registrazioni e la conservazione dei log nella misura e per il periodo previsti dalla normativa applicabile e dalle esigenze di sicurezza, accountability e tutela dei diritti.

13. FRIA E DPIA

FRIA e DPIA costituiscono valutazioni distinte, pur potendo essere coordinate per evitare duplicazioni e assicurare un'analisi integrata dei rischi.

La **FRIA** è effettuata nei casi previsti dall'articolo 27 AI Act e valuta gli effetti dell'utilizzo del sistema sui diritti fondamentali delle persone interessate.

La **DPIA** è effettuata nei casi previsti dall'articolo 35 GDPR, in particolare quando il trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

La necessità di una FRIA non determina automaticamente la necessità di una DPIA e viceversa.

Qualora entrambe risultino necessarie, esse sono coordinate in modo da assicurare coerenza delle valutazioni, ferma restando la distinta base normativa.

Il RPD/DPO fornisce la consulenza prevista dal GDPR in materia di DPIA e può essere consultato, per i profili di protezione dei dati personali, nel procedimento complessivo di valutazione del sistema IA.

14. PROTEZIONE DEI DATI PERSONALI

Il trattamento di dati personali mediante sistemi IA deve rispettare i principi di liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione, esattezza, limitazione della conservazione, integrità, riservatezza e responsabilizzazione.

Prima dell'attivazione devono essere individuati:

finalità del trattamento; base giuridica; categorie di dati; categorie di interessati; soggetti autorizzati; eventuali responsabili e sub-responsabili; trasferimenti verso Paesi terzi; tempi di conservazione; misure di sicurezza; eventuali obblighi informativi; modalità di esercizio dei diritti.

L'Ente privilegia configurazioni che escludano, ove tecnicamente disponibili e compatibili con le finalità, l'utilizzo dei dati dell'Amministrazione per addestrare, riaddestrare o migliorare modelli destinati a finalità proprie del fornitore.

È vietato utilizzare dati personali per addestrare o personalizzare autonomamente sistemi o modelli IA senza specifica preventiva valutazione e autorizzazione.

I principi di protezione dei dati fin dalla progettazione e per impostazione predefinita devono essere applicati durante l'intero ciclo di vita del sistema.

15. SICUREZZA, CYBERSECURITY E LOGGING

I sistemi IA devono essere inclusi nel sistema di gestione dei rischi ICT e di cybersecurity dell'Ente.

Prima dell'attivazione devono essere valutati almeno:

sicurezza degli accessi; autenticazione; privilegi; segregazione dei ruoli; protezione delle API; cifratura; sicurezza dei dati; gestione delle vulnerabilità; dipendenze software; supply chain; logging; backup; continuità operativa; disponibilità del servizio; gestione degli aggiornamenti; monitoraggio; rischio di prompt injection; data poisoning; model manipulation; data leakage e ulteriori rischi pertinenti alla soluzione.

L'Ente assicura che i log siano pertinenti, protetti da accessi e alterazioni non autorizzate e conservati per periodi proporzionati alle finalità e agli obblighi applicabili.

Il logging non deve determinare una raccolta indiscriminata di dati personali.

Le modalità di conservazione dei log devono essere coordinate con le policy generali dell'Ente in materia di sicurezza, protezione dei dati e gestione degli eventi.

16. RAPPORTI CON FORNITORI E PROCUREMENT

L'acquisizione di soluzioni IA deve essere preceduta da una valutazione delle esigenze dell'Ente e dei rischi connessi al ciclo di vita del sistema.

Nei capitolati, contratti, accordi o ordini devono essere introdotte, in funzione del caso concreto, disposizioni relative a:

ruolo del fornitore ai sensi dell'AI Act; classificazione del sistema; conformità normativa; documentazione tecnica; livelli di servizio; accuratezza e prestazioni; aggiornamenti del modello; modifiche sostanziali; interoperabilità; portabilità; reversibilità; contrasto al vendor lock-in; cybersecurity; gestione delle vulnerabilità; incident reporting; audit; logging; trattamento e localizzazione dei dati; trasferimenti internazionali; utilizzo dei dati per addestramento o miglioramento dei modelli; proprietà intellettuale; subfornitori; cancellazione o restituzione dei dati; dismissione; continuità del servizio.

Qualora il fornitore tratti dati personali per conto dell'Ente devono essere soddisfatti i requisiti dell'articolo 28 GDPR.

Il fornitore deve comunicare preventivamente modifiche significative del sistema, del modello, delle condizioni di utilizzo o della catena di subfornitura che possano incidere sulla valutazione originariamente effettuata.

L'Ente deve conservare un adeguato controllo sulla soluzione e sulla capacità di valutarne il comportamento nel tempo.

Eventuali clausole di manleva non fanno venir meno le responsabilità che la normativa attribuisce direttamente all'Ente.

17. RAPPORTI CON I LAVORATORI

L'utilizzo dell'IA nella gestione del personale deve rispettare la normativa europea e nazionale, il GDPR, lo Statuto dei lavoratori, la contrattazione collettiva e le ulteriori disposizioni applicabili.

È vietato utilizzare sistemi IA per forme di controllo occulto o per trattamenti incompatibili con i diritti e le libertà dei lavoratori.

Prima di utilizzare sul luogo di lavoro un sistema IA ad alto rischio, l'Ente assicura gli adempimenti informativi nei confronti dei rappresentanti dei lavoratori e dei lavoratori interessati previsti dall'AI Act, ferme le ulteriori garanzie previste dall'ordinamento nazionale.

Gli strumenti IA destinati a supportare reclutamento, selezione, assegnazione di compiti, valutazione, promozione, gestione o cessazione del rapporto di lavoro sono sottoposti a specifica valutazione preventiva.

L'utilizzo di categorie particolari di dati personali dei lavoratori deve essere limitato ai casi consentiti dalla normativa e alle finalità strettamente necessarie.

18. TRASPARENZA VERSO CITTADINI E UTENTI

Quando previsto dalla normativa, l'Ente informa le persone dell'interazione con un sistema IA in modo chiaro, comprensibile e accessibile.

I chatbot e gli assistenti virtuali rivolti al pubblico devono consentire all'utente di comprendere che sta interagendo con un sistema artificiale, salvo che ciò risulti evidente dal contesto.

Devono essere previsti canali adeguati per rivolgersi a personale umano quando la natura del servizio, i diritti interessati o il rischio del sistema lo richiedano.

L'Ente assicura la trasparenza sull'impiego dell'IA nell'azione amministrativa nei limiti previsti dalla normativa, salvaguardando al contempo sicurezza, segreti, proprietà intellettuale e altri interessi giuridicamente tutelati.

Le informative sul trattamento dei dati personali sono aggiornate quando l'utilizzo dell'IA determina modifiche rilevanti rispetto alle informazioni precedentemente rese.

19. ALFABETIZZAZIONE, FORMAZIONE E COMPETENZE

L'Ente assicura, ai sensi dell'articolo 4 AI Act, un livello adeguato di alfabetizzazione in materia di IA del personale e degli altri soggetti che utilizzano sistemi IA per conto dell'Amministrazione.

La formazione è proporzionata alle funzioni esercitate, al livello di rischio dei sistemi e alle conoscenze ed esperienze dei destinatari.

Sono previsti, ove opportuno, livelli formativi differenziati:

formazione di base per il personale; formazione operativa per gli utilizzatori di sistemi autorizzati; formazione specialistica per RTD, ICT, procurement, Referente IA e soggetti coinvolti nella governance; formazione specifica per gli addetti alla supervisione di sistemi ad alto rischio.

La formazione riguarda almeno i limiti dell'IA, le allucinazioni, i bias, la sicurezza, la protezione dei dati, l'uso dei prompt, la verifica degli output, gli obblighi di trasparenza e le modalità di segnalazione degli incidenti.

La partecipazione alle attività obbligatorie è documentata.

20. MONITORAGGIO, AUDIT E RIESAME DEI SISTEMI

L'autorizzazione all'utilizzo di un sistema IA non esaurisce gli obblighi di controllo dell'Ente.

I sistemi autorizzati sono sottoposti a monitoraggio proporzionato al rischio.

Il monitoraggio considera, ove applicabile:

accuratezza; tasso di errore; reclami; incidenti; bias; disponibilità; sicurezza; variazioni delle prestazioni; aggiornamenti del fornitore; mutamenti del contesto di utilizzo; efficacia della supervisione umana; conformità delle modalità di trattamento dei dati.

I sistemi a maggiore rischio sono sottoposti a riesame periodico formalizzato.

Deve essere effettuata una nuova valutazione prima dell'introduzione di modifiche sostanziali relative a finalità, dati trattati, modello, provider, integrazioni, destinatari, autonomia o modalità di utilizzo.

L'Ente può svolgere audit specifici, anche mediante soggetti indipendenti, in funzione della rilevanza del sistema.

21. GESTIONE DEGLI INCIDENTI IA

L'Ente integra gli incidenti connessi ai sistemi IA nel proprio sistema generale di incident management.

Qualsiasi anomalia significativa, output gravemente errato, utilizzo non autorizzato, compromissione, perdita di dati, comportamento discriminatorio, malfunzionamento o altro evento potenzialmente idoneo a produrre danni deve essere tempestivamente segnalato attraverso i canali interni individuati dall'Ente.

La gestione dell'incidente comprende, ove necessario:

contenimento; sospensione cautelativa; raccolta delle evidenze; analisi tecnica; valutazione degli impatti; coinvolgimento delle funzioni competenti; ripristino; azioni correttive; documentazione; riesame delle misure adottate.

Quando l'incidente costituisce anche una violazione di dati personali, si applica la procedura di data breach dell'Ente e gli articoli 33 e 34 GDPR.

Quando ricorrono le condizioni previste dall'AI Act per la gestione o comunicazione di incidenti gravi, sono applicate le relative disposizioni.

L'Ente adotta o integra un **AI Incident Response Plan**, coordinato con i piani di cybersecurity, business continuity e data breach management.

22. SEGNALAZIONI E WHISTLEBLOWING

Le anomalie e le violazioni ordinarie della presente Politica sono segnalate attraverso i canali organizzativi e di incident management individuati dall'Ente.

L'utilizzo del canale whistleblowing è riservato alle segnalazioni che presentano i requisiti e rientrano nell'ambito di applicazione del d.lgs. 10 marzo 2023, n. 24.

La gestione delle segnalazioni whistleblowing rimane separata dal normale processo di gestione degli incidenti IA e deve assicurare le specifiche garanzie di riservatezza previste dalla normativa.

L'eventuale coinvolgimento di ulteriori funzioni dell'Ente da parte del gestore della segnalazione deve avvenire nel rispetto dei principi di necessità e riservatezza.

23. VIOLAZIONI DELLA POLITICA E RESPONSABILITÀ

La violazione della presente Politica può assumere rilevanza disciplinare, contrattuale, amministrativa, civile o penale nei casi previsti dalla normativa.

Le eventuali misure disciplinari nei confronti del personale sono valutate e applicate esclusivamente secondo le disposizioni legislative, regolamentari e contrattuali vigenti, il Codice di comportamento e il Codice disciplinare applicabile.

La presente Politica non introduce autonomamente nuove fattispecie disciplinari.

Nei confronti di fornitori, consulenti e collaboratori trovano applicazione le misure e le conseguenze previste dai rispettivi contratti e dalla legge.

24. DISMISSIONE DEI SISTEMI

La dismissione di un sistema IA deve essere pianificata e documentata.

Devono essere valutati almeno:

esportazione e restituzione dei dati; cancellazione dei dati presso il fornitore; cancellazione o revoca delle credenziali; conservazione della documentazione necessaria; continuità del servizio; migrazione verso altri sistemi; conservazione dei log nei termini applicabili; chiusura delle integrazioni; aggiornamento del Registro IA.

Il fornitore deve attestare, ove previsto contrattualmente o necessario, l'avvenuta cancellazione dei dati e delle relative copie.

25. REVISIONE E AGGIORNAMENTO

La presente Politica è sottoposta a riesame periodico e comunque quando intervengano modifiche significative del quadro normativo, regolamentare, tecnologico od organizzativo.

La revisione è valutata, in particolare, in occasione dell'aggiornamento del Piano Triennale per l'Informatica nella Pubblica Amministrazione, degli strumenti di programmazione dell'Ente, dell'emanazione o modifica di Linee guida delle autorità competenti, dell'entrata in vigore di nuovi obblighi dell'AI Act, dell'introduzione di nuove categorie di sistemi IA o dell'emersione di incidenti significativi.

Le proposte di aggiornamento possono essere formulate dal RTD, dalle strutture competenti, dal Referente IA, dal RPD/DPO per gli aspetti di propria competenza, dal RPCT o dagli altri soggetti istituzionali coinvolti.

Le modifiche sono adottate dall'organo competente nel rispetto dei ruoli e delle responsabilità previsti dall'ordinamento.

26. PUBBLICAZIONE E DIFFUSIONE

La Politica è portata a conoscenza di tutto il personale e dei soggetti tenuti alla sua osservanza.

Essa è resa disponibile attraverso i canali interni dell'Ente e, ove ritenuto opportuno o previsto dalla normativa, pubblicata sul sito istituzionale.

Le disposizioni rilevanti sono richiamate negli atti, nei capitoli e nei contratti relativi a sistemi IA.

La Politica è trasmessa almeno al Segretario Generale, ai dirigenti e responsabili, al RTD, alla struttura ICT/Cybersecurity, al RPD/DPO, al RPCT, all'Ufficio Personale, all'Ufficio Gare e Contratti e alle ulteriori strutture interessate.

ALLEGATO 1 – SCHEDA DI RICHIESTA E AUTORIZZAZIONE DI UN SISTEMA IA

Struttura proponente: _____

Responsabile: _____

Sistema/prodotto: _____

Fornitore: _____

Versione/modello: _____

Finalità istituzionale: _____

Descrizione del caso d'uso: _____

Categorie di utenti: _____

Persone sulle quali può incidere il sistema: _____

Dati utilizzati: _____

Sono trattati dati personali? SÌ / NO

Categorie particolari di dati personali? SÌ / NO

Dati ex art. 10 GDPR? SÌ / NO

Fonti dei dati: _____

Output prodotti: _____

Il sistema supporta decisioni su persone? SÌ / NO

Livello di autonomia: _____

Modalità di supervisione umana: _____

Possibile pratica vietata ex art. 5 AI Act: SÌ / NO / DA VALUTARE

Possibile sistema ad alto rischio: SÌ / NO / DA VALUTARE

Obblighi di trasparenza ex AI Act: SÌ / NO / DA VALUTARE

DPIA necessaria: SÌ / NO / DA VALUTARE

FRIA necessaria: SÌ / NO / DA VALUTARE

Valutazione cybersecurity eseguita: SÌ / NO

Responsabile ex art. 28 GDPR: SÌ / NO / NON APPLICABILE

Dati utilizzati dal provider per training/miglioramento: SÌ / NO / DA VERIFICARE

Trasferimenti extra SEE: SÌ / NO / DA VERIFICARE

Misure di logging: _____

Misure di sicurezza: _____

Data valutazione: _____

Esito: AUTORIZZATO / AUTORIZZATO CON PRESCRIZIONI / NON AUTORIZZATO / NECESSARIA ULTERIORE ISTRUTTORIA

Prescrizioni: _____

Data prevista per il riesame: _____

ALLEGATO 2 – CHECKLIST MINIMA AI ACT – GDPR – CYBERSECURITY – PROCUREMENT

Prima dell'autorizzazione deve essere verificato, almeno ove pertinente:

AI ACT

- natura del sistema;
- ruolo dell'Ente;
- pratiche vietate;
- classificazione high-risk;
- obblighi di trasparenza;
- human oversight;
- FRIA;
- logging;
- obblighi del deployer.

GDPR

- finalità;
- base giuridica;
- minimizzazione;
- informativa;
- categorie particolari di dati;
- art. 22 GDPR;
- responsabili del trattamento;
- trasferimenti internazionali;
- conservazione;
- DPIA;
- privacy by design e by default.

CYBERSECURITY

- autenticazione;
- autorizzazioni;
- logging;
- cifratura;
- API;
- vulnerabilità;
- supply chain;
- segregazione;
- backup;
- business continuity;
- incident response;
- prompt injection;
- data leakage;
- data/model poisoning.

PROCUREMENT

- qualificazione del provider;
- documentazione tecnica;
- livelli di servizio;
- accuratezza;
- aggiornamenti;
- audit;

- subfornitori;
 - utilizzo dei dati per training;
 - proprietà intellettuale;
 - portabilità;
 - reversibilità;
 - exit strategy;
 - cancellazione dei dati;
 - comunicazione delle modifiche sostanziali.
-

ALLEGATO 3 – CONTENUTI MINIMI DEL REGISTRO IA

Per ciascun sistema devono essere registrati almeno:

1. identificativo interno;
2. denominazione del sistema;
3. provider;
4. versione/modello;
5. struttura utilizzatrice;
6. responsabile interno;
7. finalità;
8. caso d'uso;
9. ruolo AI Act dell'Ente;
10. classificazione AI Act;
11. categorie di utenti;
12. categorie di persone interessate;
13. dati personali trattati;
14. categorie particolari di dati;
15. base giuridica;
16. responsabile ex art. 28 GDPR;
17. DPIA;
18. FRIA;
19. misure di human oversight;
20. obblighi di trasparenza;
21. modalità di logging;
22. misure di sicurezza;
23. data autorizzazione;
24. eventuali prescrizioni;

- 25. data ultimo riesame;
- 26. data prossimo riesame;
- 27. incidenti significativi;
- 28. modifiche sostanziali;
- 29. stato del sistema;
- 30. data e modalità di dismissione.