DELIBERA DEL CONSIGLIO DI AMMINISTRAZIONE

N. 23 DEL 07.07.2026

L'anno 2026 il giorno 7 luglio alle ore 14.00 presso la sede di Via dell'Artigliere n. 9 a seguito di regolare convocazione si è riunito il Consiglio di Amministrazione dell'ESU di Verona

OGGETTO: **Adozione del "Regolamento per il corretto utilizzo dell'intelligenza artificiale" dell'ESU di Verona**

CONSIGLIERI

		P	A
1	Cau Sergio		X
2	Gottin Leonardo	X	
3	Miceli Sopo Francesco	X	
4	Valente Claudio	X	
5	----------*		

* il consigliere Facci Daniele in data 07.01.2025 ha rassegnato le dimissioni ed è in corso la procedura di nomina del nuovo rappresentante del Consiglio Regionale.

PRESIDENTE Valente Claudio

SEGRETARIO Gugole Giorgio

COLLEGIO DEI REVISORI CONTI

Dal Dosso Davide Tommaso
Gambaretto Nicola
Simonato Flavio

IL CONSIGLIO DI AMMINISTRAZIONE

Sentita la relazione del Presidente che illustra l'argomento posto all'ordine del giorno:

PREMESSO che ESU riconosce che l'intelligenza artificiale può contribuire a rendere l'azione amministrativa più efficace, tempestiva e comprensibile, a condizione che sia utilizzata con misura, competenza e piena responsabilità.

CONSIDERATO che l'intelligenza artificiale è uno strumento e come tale necessita di essere coordinato, non deve esercitare poteri pubblici e non sostituisce il giudizio delle persone chiamate a istruire, valutare e decidere.

VALUTATO che il presente regolamento disciplina l'utilizzo dei sistemi di intelligenza artificiale nell'Ente, con l'obiettivo di consentirne un impiego utile e innovativo, ma al tempo stesso conforme alla legge, rispettoso dei diritti fondamentali, sicuro per i dati e comprensibile per cittadini, imprese e personale.

CONSIDERATO che le policy si applicano a tutti gli uffici, servizi e articolazioni organizzative dell'Ente, nonché a dipendenti, dirigenti, amministratori, collaboratori, consulenti, tirocinanti, fornitori e soggetti esterni che, a qualunque titolo, utilizzino strumenti di intelligenza artificiale per finalità riconducibili all'Ente.

CONSIDERATO che il presente regolamento si adotta nel quadro della normativa europea e nazionale vigente e, in particolare, tiene conto delle seguenti fonti:

- Regolamento (UE) 2024/1689 – AI Act
- Legge 23 settembre 2025, n. 132
- Regolamento (UE) 2016/679 – GDPR e D.Lgs. 196/2003
- D.Lgs. 82/2005 – Codice dell'Amministrazione Digitale
- Legge 241/1990
- D.Lgs. 33/2013 e Legge 190/2012
- D.Lgs. 36/2023
- Legge 4/2004 e Direttiva (UE) 2016/2102
- Legge 300/1970, art. 4, e normativa lavoristica
- D.Lgs. 24/2023
- Piano Triennale per l'informatica nella PA
- Indicazioni di AgID, ACN, Garante privacy e altre autorità competenti

Tutto ciò premesso e considerato.

VISTO decreto legislativo 29 marzo 2012, n. 68;

VISTO il DPCM 9 aprile 2001;

VISTO la legge regionale 7 aprile 1998, n. 8;

Sottoposta a votazione la presente deliberazione risulta così approvata:

- Consiglieri presenti N. 3
- Consiglieri votanti N. 3
- Voti favorevoli N. 3
- Voti contrari N. =
- Astenuti N. =

D E L I B E R A

1. di considerare le premesse parte integrante del presente provvedimento;
2. di approvare il "Regolamento per il corretto utilizzo dell'intelligenza artificiale" dell'ESU di Verona;
3. di demandare al Direttore dell'ESU ogni provvedimento conseguente all'approvazione e all'attuazione della presente deliberazione;
4. di individuare quale responsabile del procedimento il Dirigente dott. Luca Bertaiola – Direzione Benefici e Servizi agli Studenti dell'ESU di Verona;
5. di trasmettere il presente provvedimento al responsabile del servizio "Albo on line" per i provvedimenti di competenza;

Atto non soggetto a controllo ai sensi della Legge Regionale 7 aprile 1998, n.8.

IL SEGRETARIO
(dott. Giorgio Gugole)

Direttore
GIORGIO
GUGOLE
ESU DI
VERONA

IL PRESIDENTE
(dott. Claudio Valente)

Presidente
CLAUDIO
VALENTE
ESU DI
VERONA

UFFICIO RAGIONERIA

Visto ed assunto l'impegno di €. _____ sul cap. _____

del Conto [R] / [C] del Bilancio _____

al n. _____ ai sensi dell'art. 43 L.R. 29.11.2001 n.39

Verona, _____

IL RAGIONIERE

_____

SEGRETERIA

Si attesta che la presente delibera, di cui questa è copia conforme all'originale per uso amministrativo, è stata trasmessa in data odierna all'Amministrazione Regionale.

Verona, _____ IL DIRETTORE

_____

La presente delibera è divenuta esecutiva a seguito di controllo da parte della Giunta Regionale in data _____.

Verona, _____ IL DIRETTORE

_____

La presente delibera è pubblicata all'albo ufficiale dell'Ente dal giorno _____.

IL DIRETTORE

_____

REGOLAMENTO PER IL CORRETTO UTILIZZO DELL'INTELLIGENZA ARTIFICIALE

Ente	ESU di Verona
Approvazione	Delibera del Consiglio di Amministrazione n. 23 del 7 luglio 2026___
Decorrenza	[Data di entrata in vigore]
Responsabile del documento	Responsabile Transizione Digitale
Revisione	Annuale o in caso di modifiche normative, organizzative o tecnologiche rilevanti

Indice

1. Premessa e finalità

L'Ente riconosce che l'intelligenza artificiale può contribuire a rendere l'azione amministrativa più efficace, tempestiva e comprensibile, a condizione che sia utilizzata con misura, competenza e piena responsabilità.
L'intelligenza artificiale è uno strumento e come tale necessita di essere coordinato, non deve esercitare poteri pubblici e non sostituisce il giudizio delle persone chiamate a istruire, valutare e decidere.
Il principio è sancito dall'Ai-Act Regolamento UE 1689-2024 dove viene rimarcato il principio *Human-Centered Design* (HCD) e il principio *Human-in-the-Loop* (HITL) che integra l'intelligenza umana nel ciclo di vita dell'IA, mantenendo una supervisione attiva per garantire accuratezza, etica e responsabilità
Il presente regolamento disciplina l'utilizzo dei sistemi di intelligenza artificiale nell'Ente, con l'obiettivo di consentirne un impiego utile e innovativo, ma al tempo stesso conforme alla legge, rispettoso dei diritti fondamentali, sicuro per i dati e comprensibile per cittadini, imprese e personale.
Le policy che vengono stabilite hanno natura di regolamentare le attività e i processi operativi che utilizzano l'IA.
Vengono integrate e contestualizzate le disposizioni in materia di protezione dei dati personali, sicurezza informatica, procedimento amministrativo, trasparenza, accessibilità, anticorruzione, gestione documentale e uso degli strumenti informatici.
Il principio guida è quello che considera l'intelligenza artificiale come un ottimo assistente che opera a fianco dei dipendenti dell'Ente senza sostituirne l'operato direttamente. Ogni scelta amministrativa deve restare riconducibile a una persona fisica competente, responsabile e identificabile.

2. Ambito di applicazione

La presente policy si applica a tutti gli uffici, servizi e articolazioni organizzative dell'Ente, nonché a dipendenti, dirigenti, amministratori, collaboratori, consulenti, tirocinanti, fornitori e soggetti esterni che, a qualunque titolo, utilizzino strumenti di intelligenza artificiale per finalità riconducibili all'Ente.
Rientrano nell'ambito della policy sia gli strumenti acquistati o sviluppati dall'Ente, sia le funzionalità di intelligenza artificiale integrate in piattaforme, applicativi gestionali, motori di ricerca, strumenti di produttività, servizi cloud, chatbot, sistemi di analisi documentale, strumenti di comunicazione, software di videosorveglianza intelligente o altri servizi digitali.
La policy si applica anche agli usi sperimentali o occasionali. L'uso "di prova" di uno strumento IA non autorizza il caricamento di dati personali, documenti interni, credenziali, informazioni riservate o contenuti non pubblici dell'Ente.

3. Quadro normativo di riferimento

Il presente regolamento si adotta nel quadro della normativa europea e nazionale vigente e, in particolare, tiene conto delle seguenti fonti.

Fonte	Rilevanza per la policy
Regolamento (UE) 2024/1689 – AI Act	Stabilisce regole armonizzate sull'intelligenza artificiale. Rilevano in particolare: art. 1, finalità; art. 3, definizioni; art. 4, alfabetizzazione IA; art. 5, pratiche vietate; art. 6 e Allegato III, sistemi ad alto rischio; artt. 14, 15 e 26, supervisione umana, robustezza, sicurezza e obblighi dei deployer; art. 49, registrazione; art. 50, trasparenza; art. 113, applicazione progressiva.
Legge 23 settembre 2025, n. 132	Reca disposizioni e deleghe al Governo in materia di intelligenza artificiale. L'art. 14 disciplina l'uso dell'IA nella pubblica amministrazione, precisando che l'utilizzo deve essere strumentale e di supporto all'attività provvedimentale e che la persona conserva autonomia, potere decisionale e responsabilità.

Fonte	Rilevanza per la policy
Regolamento (UE) 2016/679 – GDPR e D.Lgs. 196/2003	Regolano il trattamento dei dati personali. Rilevano in particolare i principi di liceità, correttezza, trasparenza, minimizzazione, esattezza, sicurezza, accountability, privacy by design e by default, DPIA e disciplina delle decisioni automatizzate.
D.Lgs. 82/2005 – Codice dell'Amministrazione Digitale	Rileva per governance digitale, responsabilità del RTD, sicurezza, interoperabilità, dati pubblici, servizi digitali, riuso software, accessibilità e qualità dei sistemi informativi pubblici.
Legge 241/1990	Rileva per procedimento amministrativo, responsabile del procedimento, istruttoria, motivazione, partecipazione e accesso agli atti. L'IA non può comprimere tali garanzie.
D.Lgs. 33/2013 e Legge 190/2012	Rilevano per trasparenza, accesso civico, prevenzione della corruzione, imparzialità, pubblicazione di dati e controllo diffuso sull'azione amministrativa.
D.Lgs. 36/2023	Rileva per l'acquisizione di sistemi, piattaforme e servizi IA mediante contratti pubblici, con particolare attenzione a requisiti, sicurezza, clausole contrattuali, accessibilità e ciclo di vita del servizio.
Legge 4/2004 e Direttiva (UE) 2016/2102	Rilevano per accessibilità di siti, applicazioni, documenti digitali e servizi erogati anche mediante IA.
Legge 300/1970, art. 4, e normativa lavoristica	Rilevano quando l'uso dell'IA può comportare controllo, monitoraggio o valutazione dei lavoratori.
D.Lgs. 24/2023	Rileva per la tutela delle segnalazioni whistleblowing e il divieto di trattamenti impropri o non autorizzati delle relative informazioni.
Piano Triennale per l'informatica nella PA	Costituisce riferimento di indirizzo per trasformazione digitale, dati, interoperabilità, sicurezza, servizi digitali e adozione responsabile dell'intelligenza artificiale nella PA.
Indicazioni di AgID, ACN, Garante privacy e altre autorità competenti	Devono essere considerate nelle fasi di adozione, sviluppo, procurement, sicurezza, trattamento dati, monitoraggio e controllo dei sistemi IA.

In caso di contrasto tra la presente policy e norme imperative sopravvenute, prevale la disciplina normativa vigente. La policy deve essere aggiornata tempestivamente in presenza di modifiche del quadro europeo o nazionale, di atti delle autorità competenti o di evoluzioni tecnologiche rilevanti.

4. Definizioni essenziali

Sistema di intelligenza artificiale: sistema automatizzato progettato per operare con livelli variabili di autonomia e capace di produrre output, quali previsioni, contenuti, raccomandazioni o decisioni, che possono influenzare ambienti fisici o virtuali.
IA generativa: insieme di sistemi o modelli in grado di generare testi, immagini, audio, video, codice, sintesi, traduzioni o altri contenuti a partire da istruzioni dell'utente.
Utente - Deployer: soggetto che utilizza un sistema IA sotto la propria autorità. L'Ente, quando utilizza un sistema proprio o acquisito da terzi, opera di norma come deployer.
Fornitore: soggetto che sviluppa, immette sul mercato o mette in servizio un sistema IA o un modello di IA, anche quando integrato in un applicativo o in un servizio cloud.
Output IA: risultato prodotto dal sistema IA, inclusi testi, suggerimenti, punteggi, classificazioni, immagini, codice, sintesi o raccomandazioni.

5. Principi generali

Legalità

Ogni impiego dell'IA deve essere fondato su una finalità legittima, coerente con le competenze dell'Ente e conforme alla normativa applicabile.

Responsabilità umana

L'output dell'IA non è mai, da solo, un atto amministrativo, una motivazione, una certificazione o una decisione. La responsabilità resta in capo alla persona fisica competente.

Funzione strumentale

L'IA può semplificare, ordinare, suggerire, riassumere o supportare. Non può decidere autonomamente né determinare l'esito di un procedimento senza controllo umano significativo.

Trasparenza e conoscibilità

Quando l'IA incide sui rapporti con cittadini, imprese o dipendenti, l'Ente deve fornire informazioni chiare sull'uso del sistema, sulle finalità, sui limiti e sulla possibilità di attivare un canale di assistenza diretta con accesso all'operatore dell'Ente.

Tracciabilità

Gli utilizzi rilevanti devono essere documentati, in modo da consentire verifiche, audit, ricostruzione delle attività, gestione degli incidenti e responsabilità interne.

Protezione dei dati personali

I dati personali non devono essere trattati con i sistemi di intelligenza artificiale a meno che l'istanza non sia propria e isolata. Viene comunque prevista una DPIA sui dati in modo da permettere la corretta valutazione del rischio dovuto all'errore umano.

Sicurezza e riservatezza

L'uso dell'IA non deve esporre sistemi, credenziali, banche dati, documenti, informazioni tecniche o dati dell'Ente a rischi non controllati.

Non discriminazione

È vietato utilizzare sistemi che producano o rafforzino discriminazioni o che incidano negativamente su persone vulnerabili, categorie protette o gruppi sociali. Al fine di valutare la liceità di gestione etica è necessario stilare una FRIA (Fundamental Rights Impact Assessment - Valutazione d'Impatto sui Diritti Fondamentali) deve essere redatta dai **deployer** (utilizzatori/operatori) di sistemi di intelligenza artificiale classificati ad **alto rischio.**

Sistemi ad alto rischio

L'AI Act stabilisce requisiti e obblighi specifici per i sistemi di intelligenza artificiale considerati ad alto rischio (applicazioni usate in ambiti come la sicurezza dei prodotti, il riconoscimento biometrico, le infrastrutture critiche, l'accesso ai servizi essenziali, l'educazione, il lavoro, la giustizia). Queste misure mirano a garantire che l'uso dell'IA sia sicuro, etico e rispettoso dei diritti fondamentali

Qualità e verificabilità

Gli output devono essere verificati con fonti attendibili e aggiornate. Le risposte dell'IA possono contenere errori, omissioni, semplificazioni improprie o riferimenti inesistenti.

Accessibilità e inclusione

L'IA non deve creare barriere nei servizi pubblici e deve essere adottata in modo coerente con le norme sull'accessibilità digitale e sull'inclusione.

6. Governance interna e responsabilità

La governance dell'intelligenza artificiale è organizzata in modo da assicurare controllo preventivo, uso proporzionato, responsabilità chiare e aggiornamento costante.

Soggetto / funzione	Compiti nella gestione dell'IA
Organi di indirizzo politico-amministrativo	Definiscono indirizzi generali, priorità e obiettivi di innovazione, senza interferire con responsabilità tecniche, istruttorie e gestionali.
Segretario generale / Direzione generale	Assicura il raccordo tra legalità, organizzazione, controlli interni e applicazione uniforme della policy.
Dirigenti e responsabili di servizio	Autorizzano e vigilano sugli usi nei rispettivi uffici, assicurando che il personale sia formato e che gli output siano verificati.
Responsabile per la Transizione Digitale	Coordina la governance digitale, cura il registro degli utilizzi IA, valuta coerenza con CAD, Piano Triennale e architettura digitale dell'Ente.
Responsabile ICT / sicurezza informatica	Valuta sicurezza, accessi, integrazioni, cloud, logging, continuità operativa, vulnerabilità e rischi tecnici.
DPO/RPD	È coinvolto quando l'uso dell'IA comporta o può comportare trattamento di dati personali, profilazione, decisioni automatizzate, DPIA o rischi elevati per gli interessati.
RPCT	Valuta profili di trasparenza, imparzialità, anticorruzione, opacità decisionale, conflitti di interesse e rischio di uso distorto dei sistemi.
Responsabile del procedimento	Resta responsabile dell'istruttoria, della motivazione e dell'esito del procedimento, anche quando si avvale del supporto dell'IA.
Dipendenti e collaboratori	Utilizzano solo strumenti autorizzati, non inseriscono dati non consentiti, verificano gli output e segnalano errori o incidenti.

7. Classificazione degli utilizzi

Prima dell'adozione o dell'utilizzo stabile di un sistema IA, l'Ente classifica il caso d'uso in base alla finalità, ai dati trattati, agli effetti sugli interessati, al livello di autonomia del sistema e al rischio per diritti, libertà e interessi pubblici.

7.1 Utilizzi ordinari a rischio minimo o limitato

- correzione linguistica, miglioramento della chiarezza e riformulazione di testi non riservati;
- predisposizione di bozze, scalette, check-list e promemoria interni;
- sintesi di documenti pubblici o già destinati alla pubblicazione;
- traduzioni di lavoro, non aventi valore ufficiale;
- supporto alla formazione del personale e alla preparazione di materiali divulgativi.

7.2 Utilizzi a rischio organizzativo o medio

- chatbot informativi o assistenti virtuali rivolti al pubblico;
- strumenti di ricerca semantica su archivi documentali dell'Ente;
- classificazione, smistamento o protocollazione assistita;
- analisi di dati amministrativi aggregati o anonimizzati;
- supporto istruttorio che non determina l'esito del procedimento.

Tali utilizzi richiedono autorizzazione interna, valutazione privacy ove pertinente, valutazione di sicurezza e registrazione nel Registro IA.

7.3 Utilizzi potenzialmente ad alto rischio

- accesso a contributi, prestazioni sociali, agevolazioni, servizi essenziali o graduatorie;

- reclutamento, gestione, valutazione o monitoraggio del personale;
- servizi educativi, sociali, sanitari, assistenziali o rivolti a soggetti vulnerabili;
- sistemi di scoring, profilazione, previsione del rischio o prioritarizzazione di persone fisiche;
- polizia locale, sicurezza urbana, controlli, sanzioni o attività ispettive;
- biometria, riconoscimento facciale, categorizzazione biometrica o riconoscimento delle emozioni.

Questi utilizzi non possono essere avviati senza valutazione preventiva rafforzata, coinvolgimento delle funzioni competenti, verifica della classificazione ai sensi dell'AI Act e adozione di misure documentate di mitigazione del rischio.

8. Regole per l'uso quotidiano

Ogni persona che utilizza strumenti IA per finalità dell'Ente deve attenersi alle seguenti regole operative. Esse valgono anche quando lo strumento è facilmente accessibile online, integrato in software d'ufficio o disponibile con account personale.

1. Utilizzare esclusivamente strumenti autorizzati o comunque ammessi dall'Ente per lo specifico caso d'uso.
2. Non inserire dati personali, dati particolari, dati giudiziari, documenti interni o informazioni riservate in strumenti non autorizzati.
3. Non inserire password, credenziali, token, chiavi API, configurazioni tecniche, log o informazioni sulla sicurezza dei sistemi.
4. Verificare sempre l'output prima di usarlo, pubblicarlo, inviarlo, protocollarlo o inserirlo in un atto.
5. Non utilizzare l'IA come fonte normativa ufficiale: norme, giurisprudenza, circolari, dati, importi e scadenze devono essere verificati su fonti istituzionali.
6. Non attribuire all'IA decisioni, responsabilità, valutazioni discrezionali o motivazioni dell'Ente.
7. Segnalare tempestivamente errori gravi, output discriminatori, fughe di dati, anomalie tecniche o utilizzi impropri.
8. Utilizzare un linguaggio istituzionale e non pubblicare contenuti generati dall'IA senza revisione dell'ufficio competente.

9. Utilizzi consentiti

Sono consentiti, nel rispetto della presente policy e previa verifica umana, gli usi di seguito indicati.

9.1 Supporto redazionale e comunicativo

L'IA può aiutare a predisporre bozze di comunicazioni, avvisi, testi informativi, FAQ, newsletter, schede di servizio, materiali formativi e versioni semplificate di testi amministrativi. La pubblicazione o trasmissione resta subordinata alla verifica dell'ufficio competente.

9.2 Supporto istruttorio non decisorio

L'IA può essere utilizzata per organizzare documenti, individuare elementi ricorrenti, predisporre check-list, riassumere fonti già verificate o evidenziare punti di attenzione. Non può determinare automaticamente l'esito dell'istruttoria né sostituire la motivazione del provvedimento.

9.3 Supporto ai servizi digitali

L'IA può essere impiegata in chatbot, assistenti virtuali, motori di ricerca evoluti e strumenti di orientamento dell'utente, a condizione che il cittadino sia informato dei limiti del servizio e possa rivolgersi a un operatore umano.

9.4 Supporto tecnico

L'IA può supportare la scrittura di codice, la documentazione tecnica, l'analisi di errori e attività di sicurezza difensiva. Il codice o le indicazioni generate devono essere verificate da personale competente prima dell'impiego in ambienti di produzione.

10. Utilizzi vietati o soggetti ad autorizzazione rafforzata

Sono vietati gli usi contrari all'art. 5 dell'AI Act, alle norme nazionali, alla protezione dei dati personali, alla sicurezza dell'Ente o ai principi di imparzialità, buon andamento e responsabilità umana.

- decisioni amministrative interamente automatizzate, prive di intervento umano significativo;
- attribuzione automatica di benefici, punteggi, graduatorie, priorità o dinieghi che incidano su persone fisiche o giuridiche;
- social scoring, valutazioni reputazionali generalizzate o profilazioni non previste dalla legge;
- uso di IA per controllare, valutare o monitorare i lavoratori senza i presupposti e le garanzie previste dalla normativa;
- riconoscimento delle emozioni in ambito lavorativo o educativo;
- categorizzazione biometrica o riconoscimento facciale in assenza di base giuridica, autorizzazione e valutazione rafforzata;
- generazione o diffusione di deepfake, contenuti manipolativi, ingannevoli o lesivi della dignità delle persone;
- caricamento di fascicoli, atti riservati, dati di minori, dati sociali, sanitari, giudiziari o disciplinari in strumenti non autorizzati;
- uso di sistemi IA per aggirare misure di sicurezza, procedure interne, controlli o obblighi di trasparenza.

Gli usi non espressamente vietati ma incidenti su diritti fondamentali, dati personali, lavoro, servizi essenziali o attività redazionali di provvedimenti richiedono preventiva autorizzazione rafforzata e documentata.

11. IA nei procedimenti amministrativi

Nel procedimento amministrativo l'IA può svolgere una funzione di ausilio, ma non può assumere decisioni finali senza previo controllo autorizzatorio. Ogni atto deve rimanere comprensibile, motivato, verificabile e imputabile all'organo o al responsabile competente.
Quando l'IA è utilizzata in una fase istruttoria rilevante, il responsabile del procedimento valuta se darne evidenza nel fascicolo, indicando lo strumento utilizzato, la finalità, il tipo di supporto richiesto, le verifiche effettuate e l'eventuale incidenza sull'attività istruttoria.
La motivazione del provvedimento non può consistere nel mero richiamo all'output di un sistema IA. Essa deve esporre le ragioni giuridiche, tecniche e fattuali della decisione, sulla base di atti, dati e fonti verificabili.

12. IA nei rapporti con cittadini e imprese

Nei servizi rivolti al pubblico, l'Ente deve evitare che l'utente attribuisca all'IA un valore ufficiale che essa non possiede. L'utente deve poter comprendere quando interagisce con un sistema automatizzato e deve sapere come ottenere assistenza umana.

- indicare chiaramente che il servizio utilizza IA;
- specificare che le risposte hanno valore informativo, salvo diversa validazione formale dell'Ente;
- mettere a disposizione un canale umano alternativo;
- registrare e correggere gli errori ricorrenti;

- aggiornare periodicamente le basi informative del sistema;
- garantire accessibilità, semplicità linguistica e non discriminazione;
- evitare che il chatbot raccolga più dati del necessario.

Avviso consigliato per chatbot o assistenti virtuali
Stai interagendo con un assistente virtuale basato su intelligenza artificiale. Le risposte hanno finalità informative e di orientamento e non costituiscono provvedimento amministrativo, certificazione, parere legale o comunicazione ufficiale dell'Ente. Per situazioni specifiche o per esercitare diritti e facoltà previsti dalla legge, puoi rivolgerti all'ufficio competente (email, telefono ecc.) .

13. Privacy e protezione dei dati personali

L'uso dell'IA che comporta trattamento di dati personali deve essere valutato prima dell'avvio. Il principio di accountability impone all'Ente di documentare le scelte, dimostrare la conformità e adottare misure adeguate al rischio.
Prima di utilizzare dati personali in sistemi IA, l'ufficio proponente, con il supporto delle funzioni competenti, stila una relazione di verifica per gli aspetti in elenco:

- finalità e necessità del trattamento;
- base giuridica;
- categorie di dati e di interessati;
- eventuale presenza di dati particolari o giudiziari;
- minimizzazione e possibilità di anonimizzazione o pseudonimizzazione;
- ruolo del fornitore e necessità di nomina a responsabile del trattamento;
- localizzazione dei dati e trasferimenti extra UE;
- tempi di conservazione;
- misure di sicurezza;
- informativa agli interessati;
- necessità di DPIA ai sensi dell'art. 35 GDPR;
- eventuale applicazione dell'art. 22 GDPR sulle decisioni automatizzate con output controllato dall'operatore umano.

14. Sicurezza informatica e riservatezza

La sicurezza è condizione essenziale per l'uso lecito e affidabile dell'IA. Ogni integrazione con sistemi dell'Ente, banche dati, archivi documentali o servizi cloud deve essere autorizzata e valutata dal punto di vista tecnico, organizzativo e contrattuale.

- è vietato utilizzare account personali per trattare informazioni dell'Ente mediante IA;
- è vietato installare estensioni, plugin o componenti IA non autorizzati;
- è vietato collegare strumenti IA a repository, banche dati, caselle di posta o cartelle condivise senza valutazione preventiva;
- devono essere definiti profili di accesso, log, conservazione, cancellazione, backup e responsabilità;
- ogni incidente deve essere gestito secondo le procedure interne e, se necessario, con il coinvolgimento del DPO/RPD e delle autorità competenti.

15. Acquisto, sviluppo e contratti

L'acquisto, lo sviluppo o l'adozione di sistemi IA deve essere preceduto da una valutazione di necessità, proporzionalità, sicurezza, sostenibilità, accessibilità e conformità normativa. L'Ente evita soluzioni opache, non auditabili o non compatibili con le proprie responsabilità pubbliche.

Nei contratti relativi a sistemi IA devono essere valutate e, ove pertinenti, inserite clausole riguardanti:

- conformità ad AI Act, Legge 132/2025, GDPR, CAD e normativa applicabile;
- divieto di utilizzare dati dell'Ente per addestramento o miglioramento del modello senza autorizzazione espressa;
- localizzazione dei dati, trasferimenti extra UE e subfornitori;
- misure di sicurezza, logging, cifratura, gestione degli accessi e continuità del servizio;
- documentazione tecnica, audit, verifiche e collaborazione per DPIA o valutazioni d'impatto;
- accessibilità, interoperabilità, reversibilità e portabilità dei dati;
- gestione degli incidenti, tempi di notifica e responsabilità;
- cancellazione o restituzione dei dati alla cessazione del servizio;
- proprietà intellettuale, licenze, riuso e responsabilità sugli output.

16. Registro interno degli utilizzi IA

L'Ente istituisce un Registro interno degli utilizzi di intelligenza artificiale, aggiornato a cura del RTD o della funzione individuata dall'Ente. Il Registro non sostituisce il registro dei trattamenti privacy, ma deve essere coordinato con esso.

Campo minimo	Contenuto
Denominazione	Nome del sistema o servizio IA
Fornitore	Soggetto che eroga o sviluppa il sistema
Ufficio utilizzatore	Servizio responsabile dell'utilizzo
Finalità	Scopo specifico e base organizzativa
Categoria di rischio	Minimo, limitato, medio, potenzialmente alto rischio
Dati trattati	Tipologia di dati, presenza di dati personali, particolari o riservati
Base giuridica / atto interno	Norma, contratto, determina, autorizzazione o altro presupposto
Valutazioni effettuate	Privacy, sicurezza, accessibilità, impatto su diritti fondamentali
Supervisione umana	Soggetto responsabile della verifica degli output
Log e conservazione	Presenza, durata, accessibilità e gestione dei log
Informativa / trasparenza	Modalità di informazione verso utenti o interessati
Riesame	Data dell'ultima verifica e prossima revisione

17. Formazione e alfabetizzazione IA

L'Ente assicura un livello adeguato di alfabetizzazione in materia di IA al personale che utilizza o gestisce sistemi IA, in coerenza con l'art. 4 dell'AI Act e con la disciplina nazionale.

- concetti essenziali di IA e limiti degli strumenti generativi;
- AI Act, Legge 132/2025 e principi applicabili alla PA;
- privacy, dati personali e riservatezza;
- sicurezza informatica e uso sicuro degli strumenti;
- verifica degli output, fonti ufficiali e rischio di errori;
- bias, discriminazioni e tutela dei soggetti vulnerabili;
- uso dell'IA nei procedimenti amministrativi e nei servizi al cittadino;
- responsabilità disciplinari, amministrative e contabili.

Gli uffici che intendono avviare utilizzi a rischio medio o alto devono assicurare la formazione preventiva del personale coinvolto.

18. Trasparenza, log, audit e monitoraggio

L'Ente garantisce trasparenza interna ed esterna sugli usi rilevanti dell'IA, secondo criteri di proporzionalità, tutela della sicurezza e protezione dei dati. Gli obblighi informativi sono più stringenti

quando il sistema interagisce con persone fisiche, genera contenuti sintetici, incide su procedimenti o tratta dati personali.
Per gli usi rilevanti devono essere conservati, ove possibile e proporzionato, elementi utili a ricostruire: lo strumento utilizzato, il periodo, la finalità, l'ufficio responsabile, i dati trattati, l'output rilevante, la verifica umana svolta, gli eventuali errori e le misure correttive.
Il Registro IA e gli usi autorizzati sono oggetto di riesame almeno annuale, nonché in caso di modifiche del sistema, variazione delle finalità, incidenti, reclami, aggiornamenti normativi o indicazioni delle autorità competenti.

19. Segnalazioni, incidenti e riesame

Chiunque rilevi un uso improprio dell'IA, un errore grave, una possibile discriminazione, una violazione di dati, un contenuto manipolativo, un output pericoloso o una perdita di controllo sul sistema deve segnalarlo tempestivamente al proprio responsabile e alle funzioni competenti.
L'Ente valuta la gravità dell'evento, adotta misure di contenimento, documenta l'accaduto, informa il DPO/RPD e il responsabile ICT ove necessario e procede, nei casi previsti, alle comunicazioni o notifiche alle autorità competenti.

20. Violazioni e responsabilità

La violazione della presente policy può comportare responsabilità disciplinare, dirigenziale, amministrativo-contabile, civile, penale, privacy o contrattuale, secondo la natura e la gravità del fatto.
Sono considerate violazioni particolarmente gravi:

- caricare dati personali o riservati in strumenti non autorizzati;
- utilizzare l'IA per decisioni amministrative automatiche non autorizzate;
- occultare l'uso rilevante dell'IA in procedimenti o servizi;
- usare output non verificati in atti ufficiali;
- impiegare sistemi vietati dall'AI Act;
- utilizzare IA per controllare lavoratori senza presupposti di legge;
- omettere il coinvolgimento del DPO/RPD in trattamenti ad alto rischio;
- violare misure di sicurezza o obblighi di riservatezza.

Allegato interno: schema minimo di valutazione preventiva

Prima dell'avvio di un nuovo utilizzo IA, l'ufficio proponente compila una scheda di valutazione contenente almeno le seguenti informazioni.

Voce	Domanda guida	Esito / note
Finalità	Quale esigenza amministrativa o organizzativa si intende soddisfare?	
Necessità	L'uso dell'IA è necessario o esistono alternative meno rischiose?	
Dati	Quali dati vengono trattati? Sono presenti dati personali o riservati?	
Rischio	L'uso può incidere su diritti, servizi, benefici, graduatorie, lavoro o soggetti vulnerabili?	
Trasparenza	L'utente deve essere informato? È previsto un canale umano?	
Supervisione	Chi verifica l'output e con quali criteri?	
Sicurezza	Sono stati valutati accessi, log, conservazione, cloud, fornitori e cancellazione?	
Privacy	È necessario coinvolgere il DPO/RPD o svolgere una DPIA?	
Contratto	Il fornitore garantisce conformità, sicurezza, audit, divieto di addestramento non autorizzato e reversibilità?	
Autorizzazione	Quale responsabile approva l'avvio e con quali limiti?	

Allegato A
Regole operative, check-list e registro IA

Strumenti pratici per uffici e dipendenti

1. Come usare questo allegato

Questo allegato rende concreta la policy. Viene consegnato al personale, usato nella formazione e allegato alle istruzioni interne.

- **La regola base è:** prima di usare l'IA, capisci cosa stai inserendo, perché lo fai, chi controllerà il risultato e quale effetto potrà avere sulle persone.

2. Le dieci regole da ricordare

- **1. Usa solo strumenti autorizzati:** se lo strumento non è approvato dall'Ente, non usarlo con dati o documenti istituzionali.
- **2. Non inserire dati personali o riservati:** usa dati anonimi, sintetici o informazioni già pubbliche.
- **3. L'IA non decide:** può aiutare, ma non sostituisce istruttoria, valutazione, firma o responsabilità.
- **4. Verifica sempre:** controlla norme, importi, date, nomi e conclusioni su fonti ufficiali.
- **5. Non usare output IA come atto finale:** ogni bozza deve essere rivista dall'ufficio competente.
- **6. Proteggi credenziali e segreti tecnici:** mai inserire password, token, chiavi API, configurazioni o log riservati.
- **7. Non profilare persone:** valutazioni su cittadini, dipendenti, candidati o fornitori richiedono base giuridica e autorizzazione.
- **8. Spiega quando serve:** se l'utente interagisce con IA, deve saperlo in modo chiaro.
- **9. Segnala anomalie:** errori gravi, bias, discriminazioni, incidenti o fughe di dati vanno segnalati subito.
- **10. Nei casi dubbi fermati:** se riguarda minori, lavoratori, servizi sociali, salute, graduatorie o benefici, chiedi prima.

3. Semaforo degli utilizzi

- **Verde - normalmente consentito:** bozze generiche, scalette, testi pubblici, miglioramento linguistico. Condizione: nessun dato personale o riservato e verifica umana.
- **Giallo - usare con attenzione:** sintesi di documenti interni non riservati, supporto a istruttorie, analisi di dati aggregati. Condizione: strumento autorizzato e controllo del responsabile.
- **Arancione - autorizzazione preventiva:** chatbot al cittadino, ricerca su archivi interni, classificazione documentale, supporto a processi di servizio. Condizione: valutazione RTD/ICT/DPO e inserimento nel registro IA.

Rosso - vietato o sospeso fino a valutazione rafforzata: decisioni automatiche, profilazione, biometria, controllo lavoratori, dati sanitari o sociali. Condizione: solo se previsto da norma, autorizzato e valutato.

4. Check-list rapida prima dell'uso

- [ ] Lo strumento è autorizzato dall'Ente per questa finalità?
- [ ] Sto inserendo dati personali, riservati o documenti interni?
- [ ] Posso usare dati anonimi, sintetici o aggregati?
- [ ] Il risultato può incidere su cittadini, imprese, dipendenti o fornitori?
- [ ] L'output sarà verificato da una persona competente?
- [ ] Devo informare l'utente che viene usata IA?
- [ ] Devo coinvolgere RTD, ICT, DPO/RPD, RPCT o responsabile del procedimento?
- [ ] Questo uso deve essere registrato nel Registro IA?
- [ ] Ho verificato copyright, licenze e segreti?
- [ ] Sono in grado di spiegare l'uso dell'IA se richiesto?

5. Check-list privacy

- [ ] La finalità è istituzionale, chiara e necessaria?
- [ ] Esiste una base giuridica adeguata?
- [ ] Sono stati ridotti o evitati i dati personali non necessari?
- [ ] Sono presenti dati sanitari, sociali, minori, giudiziari, disciplinari o dei lavoratori?
- [ ] Il fornitore deve essere nominato responsabile del trattamento ex art. 28 GDPR?
- [ ] Il fornitore usa dati dell'Ente per addestrare modelli?
- [ ] Sono chiari conservazione, log, localizzazione e trasferimenti extra UE?
- [ ] Serve una DPIA?
- [ ] Gli interessati ricevono un'informativa chiara?
- [ ] Il DPO/RPD è stato coinvolto quando necessario?

6. Check-list per atti e procedimenti

- [ ] L'IA è stata usata solo come supporto e non per decidere l'esito?
- [ ] Il responsabile del procedimento ha verificato l'output?
- [ ] La motivazione dell'atto è autonoma e basata su fonti ufficiali?
- [ ] Sono stati controllati norme, importi, scadenze e competenze?
- [ ] Sono stati rimossi dati personali non necessari?
- [ ] L'uso va annotato nel fascicolo o nel registro?
- [ ] Sono garantiti partecipazione, accesso e possibilità di riesame?

7. Prompt sicuri: esempi

Riscrivere un avviso. Evita di incollare elenchi nominativi. Prompt più sicuro: 'Riscrivi in linguaggio semplice questo avviso pubblico privo di dati personali'.
Preparare FAQ. Evita di caricare domande reali con nomi e recapiti. Prompt più sicuro: 'Crea FAQ generiche sul servizio X usando solo informazioni pubbliche'.
Bozza di determina. Evita di caricare il fascicolo completo. Prompt più sicuro: 'Prepara una struttura di determina usando campi segnaposto'.
Analisi dati. Evita file con codici fiscali o indirizzi. Prompt più sicuro: 'Suggerisci indicatori per dati aggregati'.

Problema tecnico. Evita token, IP interni e log completi. Prompt più sicuro: 'Spiega in termini generali come diagnosticare un errore 500'.

8. Modulo richiesta autorizzazione strumento IA

- **Ufficio richiedente:** _____
- **Referente:** _____
- **Nome strumento e fornitore:** _____
- **Finalità d'uso:** _____
- **Utenti coinvolti:** _____
- **Dati trattati:** _____
- **Dati personali presenti? quali:** _____

Dati particolari/giudiziari/minori/lavoratori presenti? _____
Collegamento a banche dati interne? _____

- **Output atteso:** _____
- **Impatto su cittadini/dipendenti/imprese:** _____
- **Categoria di rischio proposta:** _____
- **Misure di controllo umano:** _____
- **Misure di sicurezza:** _____
- **Tempi di conservazione:** _____
- **Necessità di informativa o DPIA:** _____
- **Pareri ICT/RTD/DPO/RPCT:** _____
- **Decisione finale:** autorizzato / autorizzato con limiti / non autorizzato.

9. Registro IA - scheda minima

- **ID strumento:** _____
- **Denominazione:** _____
- **Fornitore:** _____
- **Ufficio utilizzatore:** _____
- **Finalità:** _____
- **Utenti abilitati:** _____
- **Dati trattati:** _____
- **Categoria di rischio:** minimo / limitato / medio / alto / vietato-non ammesso.
- **Base giuridica o atto interno:** _____
- **DPIA:** sì / no / da valutare. Riferimento: _____
- **Responsabile interno:** _____
- **Informativa o avviso di trasparenza:** _____
- **Log:** quali, dove e per quanto tempo: _____
- **Data autorizzazione:** _____
- **Data prossimo riesame:** _____
- **Incidenti o anomalie registrate:** _____

10. Schema di escalation

- **Dati personali inseriti per errore:** interrompere l'uso, salvare evidenze e coinvolgere responsabile, DPO/RPD e ICT.
- **Output discriminatorio o offensivo:** non usarlo, segnalarlo e verificare dati, prompt e configurazione.
- **Risposta errata pubblicata:** correggere o ritirare il contenuto e valutare un chiarimento pubblico.
- **Incidente di sicurezza:** seguire le procedure interne e coinvolgere ICT, RTD e DPO/RPD.
- **Uso non autorizzato in procedimento:** sospendere l'uso e rivalutare l'istruttoria con il responsabile.

11. Mini-glossario

- **Allucinazione:** risposta plausibile ma falsa o non verificata.
- **Bias:** distorsione che può portare a risultati ingiusti o discriminatori.
- **Prompt:** istruzione inviata al sistema IA.
- **Output:** risposta o risultato generato dal sistema.
- **DPIA:** valutazione d'impatto sulla protezione dei dati.
- **Log:** traccia tecnica o operativa.
- **Deepfake:** contenuto audio, video o immagine falsificato o alterato con IA.