



CAMERA DI COMMERCIO
CASERTA

Uso dei sistemi di Intelligenza Artificiale in Camera di Commercio Industria Artigianato e Agricoltura di Caserta **POLICY**





INDICE

1. PREMESSA	2
2. SCOPO	3
3. CAMPO DI APPLICAZIONE	4
4. QUADRO NORMATIVO DI RIFERIMENTO	5
5. DEFINIZIONI	6
6. PRINCIPI GUIDA	8
7. REGOLE DI UTILIZZO, GESTIONE DEL RISCHIO E VALUTAZIONE DI IMPATTO	9
8. REQUISITI DI CONFORMITA' E TRASPARENZA	11
9. GOVERNANCE, MONITORAGGIO E AGGIORNAMENTO	12
10. DOCUMENTI COLLEGATI	13



1. PREMESSA

L'intelligenza artificiale (IA) si configura oggi come una leva strategica imprescindibile per l'innovazione e il continuo miglioramento dei servizi pubblici, con significative ricadute sull'efficienza, sulla tempestività e sulla qualità complessiva delle attività.

La rapida evoluzione tecnologica che ha contraddistinto gli ultimi anni ha inciso in maniera profonda sulle modalità operative e sui paradigmi di gestione e interazione con i flussi informativi, rendendo l'IA una componente sempre più centrale nel governo di processi istituzionali complessi. L'introduzione di tali soluzioni, tuttavia, richiede un approccio metodologico rigoroso e un elevato livello di consapevolezza critica, indispensabili per assicurare che i benefici derivanti dall'innovazione siano accompagnati da un'adeguata e sistematica mitigazione dei rischi connessi.

Affinché l'intelligenza artificiale possa essere impiegata in modo realmente efficace e responsabile nella Pubblica Amministrazione, è necessario sottoporla a un articolato processo di valutazione, addestramento e monitoraggio continuo, eventualmente supportato da strumenti di supervisione, finalizzato a verificare la qualità dei contenuti generati, la coerenza delle soluzioni fornite e l'impatto concreto sulle performance organizzative. In tale prospettiva, la disponibilità di dati strutturati, interoperabili, costantemente aggiornati e di comprovata affidabilità costituisce un presupposto imprescindibile per la realizzazione di sistemi solidi, in grado di produrre informazioni corrette e di evolvere nel tempo secondo criteri di controllo, trasparenza e verificabilità. Questo orientamento consente di coniugare in modo equilibrato la spinta all'innovazione tecnologica con i doveri propri della responsabilità pubblica, promuovendo un modello di utilizzo dell'intelligenza artificiale in cui la tecnologia non si sostituisce al capitale umano, ma ne valorizza e rafforza le capacità analitiche, decisionali e operative, accrescendo il valore del servizio reso alla collettività.

Nel quadro sopra delineato, l'integrazione dell'Intelligenza Artificiale rappresenta una frontiera cruciale anche per la modernizzazione del sistema camerale. Grazie alla capacità di analizzare grandi volumi di dati, individuare pattern ricorrenti e supportare la produzione di contenuti e decisioni informate, l'intelligenza artificiale può contribuire allo sviluppo di una "Sistema camerale aumentato": un sistema in cui la tecnologia affianca i dipendenti, ne potenzia le competenze professionali e migliora l'efficacia e la qualità dei servizi erogati a cittadini e imprese, senza sostituirne il ruolo né ridurne la responsabilità.

Occorre tuttavia evitare una fascinazione acritica verso l'intelligenza artificiale. Non tutte le criticità organizzative e operative trovano infatti la loro soluzione nell'adozione di tecnologie di IA. È pertanto fondamentale valutare con attenzione in quali ambiti l'intelligenza artificiale sia effettivamente in grado di generare valore aggiunto, tenendo conto che essa non rappresenta



l'unica opzione tecnologica disponibile. In molti casi, soluzioni digitali già mature e consolidate – quali la Robotic Process Automation (RPA) per l'automazione di attività ripetitive e a basso valore aggiunto, gli strumenti di business intelligence per l'analisi strutturata dei dati o i sistemi evoluti di gestione documentale e dei flussi procedurali – possono risultare più semplici, sostenibili ed efficaci rispetto all'introduzione di soluzioni di IA.

Alla luce di tali considerazioni, l'adozione dell'intelligenza artificiale deve essere preceduta da una valutazione strutturata e consapevole delle esigenze dell'Ente, che tenga conto dei processi coinvolti, della qualità e disponibilità dei dati, dei benefici attesi, dei costi di implementazione e gestione, nonché dei rischi organizzativi, tecnologici e giuridici. Solo attraverso un'analisi comparativa tra diverse opzioni tecnologiche è possibile individuare in modo appropriato dove e come l'IA possa costituire la soluzione più adeguata e coerente con gli obiettivi strategici dell'amministrazione.

In ogni percorso di innovazione digitale, e in particolare nell'adozione di soluzioni di intelligenza artificiale, restano imprescindibili alcuni principi abilitanti. In primo luogo, la trasparenza dei processi decisionali, che deve consentire di comprendere in che modo gli strumenti digitali supportano l'azione amministrativa, evitando opacità, automatismi non governati o forme di delega impropria alla tecnologia. In secondo luogo, una governance condivisa e multilivello, che coinvolga le strutture tecniche, organizzative e giuridiche dell'Ente, assicurando un presidio costante su scelte progettuali, utilizzo dei dati, sicurezza, responsabilità e conformità normativa.

A ciò si affianca la necessità di garantire la piena interoperabilità dei sistemi informativi, in coerenza con il quadro nazionale ed europeo, affinché le soluzioni di IA non si traducano in nuove frammentazioni tecnologiche, ma si integrino efficacemente con le piattaforme e le infrastrutture esistenti. Solo in questo modo l'intelligenza artificiale può essere utilizzata come leva di innovazione sostenibile, rispettosa dei principi etici, della protezione dei dati personali, della sicurezza informatica e dell'interesse pubblico, contribuendo a rafforzare la fiducia dei cittadini e a migliorare la qualità complessiva dell'azione amministrativa.

2. SCOPO

La presente policy definisce principi, regole e responsabilità per l'utilizzo, lo sviluppo e l'acquisizione di sistemi di intelligenza artificiale all'interno della Camera di Commercio di Caserta, assicurandone l'impiego in modo etico, sicuro e conforme alla normativa vigente.

Il presente documento si prefigge lo scopo di:

- comunicare l'importanza di un'adeguata gestione dell'IA per garantire la conformità alle leggi vigenti;



- supportare ed indirizzare il personale e tutti i collaboratori della Camera di Commercio di Caserta ad un uso lecito, sicuro, affidabile, trasparente dell'IA mediante misure tecniche, organizzative ed azioni formative;
- supportare l'efficientamento dei processi dell'Ente attraverso strumenti innovativi, pur garantendo la conoscibilità del funzionamento e la tracciabilità del suo utilizzo;
- rafforzare la fiducia degli stakeholder attraverso un utilizzo dell'intelligenza artificiale conforme ai principi di tutela dei diritti fondamentali e di protezione dei dati personali, adottando un approccio di responsabilità proattiva;
- affiancare le già presenti policy per la Sicurezza delle informazioni e per la Protezione dei Dati Personali per garantire una sinergica operatività con i sistemi di IA.

La policy costituisce parte integrante del Sistema di Gestione Integrato Qualità e Sicurezza delle Informazioni della Camera di Commercio e segue le regole di aggiornamento e di gestione documentale in essi descritte. Tale documento concorre, inoltre all'attuazione di quanto disciplinato dall'art. 14, comma 3, della legge n. 132/2025 che prevede che *"Le pubbliche amministrazioni adottano misure tecniche, organizzative e formative finalizzate a garantire un utilizzo responsabile dell'intelligenza artificiale e a sviluppare le capacità trasversali degli utilizzatori."*

3. CAMPO DI APPLICAZIONE

La presente policy si applica a:

- progetti, servizi e attività che prevedono l'uso di soluzioni di intelligenza artificiale, sviluppate internamente o acquisite da terzi;
- sistemi e tecnologie di IA generativa, machine learning, analisi predittiva, automazione intelligente, chatbot, riconoscimento vocale o visivo sviluppati internamente o acquisiti da terzi;
- attività sperimentali o *proof of concept* inerenti soluzioni di intelligenza artificiale sviluppati internamente o acquisiti da terzi.

È tenuto al rispetto della presente policy il personale della Camera di Commercio di Caserta (indipendentemente dalla forma e dall'inquadramento contrattuale) e i collaboratori che a vario titolo operano con l'Ente. Il presente documento si applica a qualsiasi modalità di accesso ai sistemi di IA nel contesto dell'attività lavorativa, indipendentemente dal dispositivo utilizzato.

La Camera di Commercio si impegna a gestire i sistemi di intelligenza artificiale lungo l'intero ciclo di vita, che comprende:



- ideazione e analisi di fattibilità, con valutazione di alternative tecnologiche non basate su IA;
- progettazione o selezione del fornitore, con verifica di conformità normativa e dei requisiti etici;
- valutazione del rischio e dell'impatto (AI Ad e DPIA);
- autorizzazione formale all'adozione;
- messa in esercizio e utilizzo controllato;
- monitoraggio continuo delle prestazioni e dei rischi;
- dismissione o sostituzione del sistema, con gestione dei dati residui.

La presente policy si applica a tutte le fasi sopra descritte, che devono essere documentate e tracciabili. Per i sistemi di IA già in uso o in fase di sperimentazione, la Camera di Commercio di Caserta si impegna ad avviare le necessarie attività di ricognizione, classificazione e progressivo adeguamento ai requisiti previsti dalla presente Policy. Per i sistemi di nuova adozione, le previsioni della Policy si applicano integralmente sin dalla fase di valutazione preliminare. La Camera di Commercio di Caserta si impegna a favorire il miglioramento continuo del sistema di gestione, provvedendo ad aggiornare il presente documento alla luce delle esperienze maturate e dell'evoluzione del contesto normativo e organizzativo.

In ogni caso, il presente documento è sottoposto a revisione almeno annuale.

4. QUADRO NORMATIVO DI RIFERIMENTO

La policy è adottata in coerenza con le principali normative e indirizzi strategici nazionali ed europei in materia di trasformazione digitale e intelligenza artificiale, tra cui:

- Regolamento (UE) 2016/679 del 27 aprile 2016 del Parlamento europeo e del Consiglio, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), di seguito indicato come GDPR;
- Regolamento europeo (UE) 1689/2024 del 13 giugno 2024 del Parlamento europeo e del Consiglio, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'Intelligenza Artificiale), di seguito indicato come AI Ad;
- Decreto legislativo 30 giugno 2003, n. 196 recante "Codice in materia di protezione dei dati personali" (Codice della privacy);
- Codice dell'Amministrazione Digitale (d.lgs. 82/2005);
- Linee guida AgID in materia di intelligenza artificiale;
- Piano Triennale per l'Informatica nella Pubblica Amministrazione 2024-2026;



- Strategia Italiana per l'Intelligenza Artificiale 2024-2026;
- LEGGE 23 settembre 2025 n. 132: Disposizioni e deleghe al Governo in materia di intelligenza artificiale;
- norma ISO/IEC 27001;
- norma ISO/IEC 42001;
- norma ISO/IEC 42005.

5. DEFINIZIONI

SISTEMI DI IA	Sistema automatizzato progettato per funzionare con livelli di autonomia variabili, che può presentare adattabilità dopo la diffusione e generare output quali previsioni, contenuti, raccomandazioni o decisioni sulla base degli input ricevuti, per obiettivi espliciti o impliciti.
Modello di IA per finalità generali	Un modello di IA, anche laddove tale modello di IA sia addestrato con grandi quantità di dati utilizzando l'autosupervisione su larga scala, che sia caratterizzato da una generalità significativa e sia in grado di svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello è immesso sul mercato, e che può essere integrato in una varietà di sistemi o applicazioni a valle, ad eccezione dei modelli di IA utilizzati per attività di ricerca, sviluppo o prototipazione prima di essere immessi sul mercato.
Sistema di IA Generativa (Gen-IA)	Un sistema di IA basato su un modello per finalità generali, specificamente progettato o adattato per generare, con vari livelli di autonomia, contenuti quali testo complesso, immagini, audio, video o codice informatico in risposta a input (prompt) forniti dall'utente.
Applicazione di IA	Qualsiasi software, applicazione web o servizio di terze parti accessibile all'utente che integri o funga da interfaccia per un Sistema di IA, utilizzato a supporto dell'attività lavorativa. Rientrano in questa categoria le interfacce utente di ChatGPT, Gemini, DeepSeek o Grok.
Training del modello	Processo di apprendimento successivo all'implementazione (post-deployment), con cui il modello viene aggiornato o migliorato utilizzando i dati forniti dagli utenti durante l'uso del servizio.



Prompt	Richiesta formulata dall'utente ad un modello di intelligenza artificiale, in forma di testo o altro input (ad esempio immagini), che guida il modello nella generazione della risposta o del contenuto richiesto.
Fornitore (provider)	Soggetto che sviluppa o immette sul mercato un sistema di intelligenza artificiale
Deployer (utilizzatore)	Soggetto, pubblico o privato, che utilizza un sistema di IA, anche integrandolo nei propri sistemi, senza modificarne <i>in</i> modo significativo il funzionamento.
Sistemi ad alto rischio	Sistema che rientra nelle categorie definite dall'AI Act, art. 6.
DPIA (Data Protection Impact Assessment)	Procedura prevista dall'art. 35 del GDPR, necessaria per identificare, valutare e mitigare i rischi di un trattamento di dati personali che possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
Incidente IA	Evento relativo a un sistema di intelligenza artificiale che produce o può produrre un impatto negativo sulla salute, sulla sicurezza o sui diritti fondamentali delle persone, sulla sicurezza delle informazioni o sulla qualità dei servizi erogati dall'Ente. Comprende, a titolo esemplificativo: output discriminatori, errori fattuali rilevanti per atti o procedimenti, violazioni dei principi di trasparenza, malfunzionamenti che compromettono la disponibilità o l'integrità dei dati.
FRIA (Fundamental Rights Impact Assessment)	La Valutazione dell'Impatto sui Diritti Fondamentali di cui all'art. 27 del Regolamento (UE) 2024/1689 (AI Act). I deployer di diritto pubblico, o i soggetti privati che forniscono servizi pubblici, che utilizzano sistemi di IA ad alto rischio di cui all'Allegato III dell'AI Act, effettuano una valutazione dell'impatto sui diritti fondamentali che l'uso di tale sistema può produrre, prima di metterlo in uso.



6. PRINCIPI GUIDA

I principi per l'adozione e l'impiego di sistemi di IA sono contenuti nell'AI Act e nella Legge n. 132/2025.

Ferma restando l'osservanza degli obblighi stabiliti dalla disciplina vigente, l'impiego di sistemi di IA da parte della Camera di Commercio avviene, nel rispetto dei seguenti principi:

- a) Legalità e conformità: l'uso dell'intelligenza artificiale deve rispettare le norme vigenti (*Linee guida AgID per l'adozione dell'intelligenza artificiale nella pubblica amministrazione - art. 4, comma 2 Schema di Codice Etico*) Trasparenza: ogni utilizzo deve essere dichiarabile, documentabile e comprensibile (*Linee guida AgID per l'adozione dell'intelligenza artificiale nella pubblica amministrazione - art. 6 Schema di Codice Etico*).
- b) Controllo umano: ogni contenuto prodotto dall'intelligenza artificiale deve essere rivisto, verificato e approvato da una persona prima di poter essere utilizzato o diffuso, al fine di garantire correttezza e conformità normativa (AI Act art. 14; *Linee guida AgID per l'adozione dell'intelligenza artificiale nella pubblica amministrazione - art. 7 Schema di Codice Etico*).
- c) Tutela dei dati: è vietato condividere dati personali o riservati (*Linee guida AgID per l'adozione dell'intelligenza artificiale nella pubblica amministrazione - art. 5, comma 2 e art. 11 Schema di Codice Etico; CAD art. 51, comma 2*).
- d) Responsabilità individuale: ogni utente è responsabile dell'uso corretto dell'intelligenza artificiale (GDPR art 5, comma 2; *Linee guida AgID per l'adozione dell'intelligenza artificiale nella pubblica amministrazione - art. 13 Schema di Codice Etico*);
- e) Non discriminazione ed equità algoritmica: i sistemi di intelligenza artificiale devono essere progettati per evitare bias o trattamenti ingiusti (AI Act art. 10);
- f) Sicurezza e robustezza: i sistemi devono garantire resistenza a manipolazioni e comportamenti imprevisti (AI Act art. 15 e 16; ISO/IEC 27001 Annex A.8);
- g) Sostenibilità e impatto sociale positivo: le soluzioni di intelligenza artificiale devono promuovere un uso efficiente delle risorse, ridurre l'impatto ambientale e generare benefici concreti per cittadini e imprese, in coerenza con la *Strategia Italiana per l'Intelligenza Artificiale 2024-2026* e con *17 Piano Triennale per l'Informatica nella PA 2024-2026*, che introducono la sostenibilità economica, ambientale e sociale come principio guida della trasformazione digitale (CAD art. 1.5).

La Camera di Commercio si impegna a declinare i principi sopra enunciati in un Codice Etico per l'intelligenza artificiale, che definisca regole di comportamento specifiche per tutto il personale e i collaboratori nell'interazione con i sistemi di IA, tenendo conto delle indicazioni che saranno fornite dall'AgID e dell'evoluzione del quadro normativo e delle migliori pratiche internazionali in materia.



7. REGOLE DI UTILIZZO, GESTIONE DEL RISCHIO E VALUTAZIONE DI IMPATTO

La Camera di Commercio non può adottare né utilizzare:

- sistemi di IA a "Rischio Inaccettabile": ovvero sistemi che rientrano nelle pratiche vietate dall'art. 5 dell'AI Act.

L'elenco delle pratiche vietate è soggetto ad aggiornamento da parte del legislatore europeo. Il RTD verifica periodicamente la coerenza dei sistemi in uso con l'evoluzione dell'art. 5 dell'AI Act.

Prima dell'adozione, acquisizione o utilizzo di qualsiasi nuovo sistema di IA, la Camera di Commercio svolge una valutazione preliminare che deve attestare:

- che il sistema non rientri tra le pratiche vietate dall'art. 5 dell'AI Act;
- la classificazione del livello di rischio del sistema ai sensi dell'AI Ad (alto rischio, rischio limitato, rischio minimo);
- la conformità alle previsioni normative in materia di protezione dei dati personali (GDPR) e sicurezza informatica;
- la compatibilità con i principi guida di cui alla sezione 6 del presente documento.

Per i sistemi classificati ad alto rischio ai sensi dell'art. 6 dell'AI Act, la valutazione preliminare è integrata dalla FRIA di cui all'art. 27 dell'AI Act e, ove il trattamento coinvolga dati personali con rischio elevato per i diritti degli interessati, dalla DPIA di cui all'art. 35 del GDPR.

La valutazione preliminare e le eventuali valutazioni integrative sono documentate e conservate nel fascicolo del sistema IA. La valutazione deve essere rivista in caso di aggiornamenti significativi del software o modifiche delle funzionalità che possano alterare la classificazione di rischio del sistema.

Per i sistemi di IA ammessi, Unioncamere garantisce la trasparenza verso l'utente e il rispetto delle istruzioni del fornitore. Inoltre, l'utilizzo di tali sistemi è subordinato a una verifica periodica volta ad accertare:

- che i risultati prodotti siano pertinenti e non viziati da errori manifesti;
- che non si verifichino effetti discriminatori o lesivi per i destinatari dei servizi;
- che sia garantita la possibilità di intervento umano per correggere o scartare gli output dell'IA.

Eventuali Incidenti IA, come definiti nella sezione 5, devono essere gestiti secondo il seguente flusso minimo:



- segnalazione tempestiva al proprio dirigente e al Responsabile per la Transizione Digitale (RTD);
- classificazione della gravità dell'incidente da parte del RTD, tenendo conto dell'impatto sui diritti fondamentali, del numero di persone potenzialmente coinvolte e dell'irreversibilità del danno;
- analisi delle cause e degli impatti, con il supporto del fornitore del sistema ove necessario;
- documentazione dell'incidente e delle azioni intraprese;
- comunicazione al DPO qualora l'incidente coinvolga dati personali, e all'Agenzia per la Cybersicurezza Nazionale (ACN) ove ricorrano gli obblighi previsti dalla normativa vigente;
- analisi post-incidente e aggiornamento della valutazione del rischio.

L'ACN è designata, dall'art. 20 della Legge n. 132/2025, quale autorità di sorveglianza del mercato ai sensi dell'AI Act e punto di contatto unico con le istituzioni dell'Unione Europea, fatte salve le competenze settoriali attribuite ad altre autorità. Gli obblighi di comunicazione per incidenti relativi a sistemi di IA si aggiungono a quelli già previsti in materia di cybersicurezza.

Le modalità operative di gestione degli incidenti IA, inclusi i criteri di escalation e le tempistiche, sono definite in una procedura dedicata, coerente con la procedura di Incident Management del Sistema di Gestione Integrato (C.2.7).

In caso di rischi significativi per la salute, la sicurezza o i diritti fondamentali delle persone, la Camera di Commercio può sospendere l'utilizzo del sistema fino alla risoluzione delle criticità.

L'RTD effettua le comunicazioni formali previste per legge all'Agenzia per la Cybersecurity Nazionale, in coerenza rispetto a quanto già fatto in ottemperanza ai rischi cyber.

L'utilizzo dei sistemi ammessi deve comunque garantire:

- una valutazione del rischio specificamente riferita al sistema di IA, condotta in coerenza con la procedura di gestione dei rischi del Sistema di Gestione Integrato (PQ-C.4.5) e con la medesima metodologia di analisi ivi prevista, estesa per includere le categorie di rischio proprie dell'intelligenza artificiale. La valutazione definisce i criteri di classificazione, il metodo di analisi, le soglie di accettabilità e le misure di trattamento per ogni rischio identificato. I risultati sono registrati nel Risk Register dell'Ente;
- il mantenimento nel tempo della conformità ai requisiti di protezione dei dati personali e di tutela dei diritti fondamentali, con revisione periodica delle valutazioni di impatto (DPIA e, per i sistemi ad alto rischio, FRIA) in coerenza con l'evoluzione del sistema, dei dati trattati e del contesto di utilizzo;



- che l'addestramento o l'uso del modello non comporti la condivisione non autorizzata di dati personali di terzi, dati particolari (art. 9 GDPR) o informazioni riservate/protette da diritti di proprietà intellettuale dell'Ente.

È fatto divieto assoluto di utilizzare, per fini lavorativi, applicazioni di IA liberamente accessibili sul mercato (es. account personali gratuiti). L'utilizzo di applicazioni di IA non verificati espone Unioncamere a rischi di sicurezza, violazione di copyright e perdita di controllo sui dati. Eventuali esigenze specifiche devono essere sottoposte alla valutazione tecnica del Responsabile per la Transizione Digitale (RTD) e autorizzate formalmente.

8. REQUISITI DI CONFORMITA' E TRASPARENZA

Ogni progetto o applicativo che integri componenti di IA deve:

- indicare chiaramente se e come integra elementi di **IA**;
- essere conforme alle norme sulla sicurezza informatica e sulla privacy;
- garantire tracciabilità e verificabilità dei risultati;
- mantenere documentazione tecnica e operativa accessibile per audit interni ed esterni. Per

gli sistemi di IA forniti da soggetti esterni, i contratti devono prevedere clausole su:

- garanzie sulla conformità alle normative applicabili (inclusi gli aspetti di protezione dati, proprietà intellettuale e sicurezza informatica);
- clausole chiare sulla non utilizzazione dei dati di Unioncamere per l'addestramento dei modelli terzi (ove applicabile);
- garanzie di continuità operativa, assistenza tecnica e aggiornamento periodico;
- obblighi di collaborazione del fornitore con il deployer per l'adempimento degli obblighi previsti dall'AI Act, inclusi: la messa a disposizione della documentazione tecnica necessaria per le valutazioni di impatto e di rischio, l'informazione tempestiva in caso di modifiche significative del sistema, e il supporto in caso di richieste da parte delle autorità di sorveglianza del mercato.

I contenuti, le analisi e le raccomandazioni prodotte da sistemi di intelligenza artificiale:

- non possono essere utilizzati direttamente in atti ufficiali, se non validati da un operatore umano;
- devono essere sempre verificati da personale competente prima di essere diffusi o utilizzati in processi decisionali.



Per la predisposizione di atti amministrativi, provvedimenti o documenti a rilevanza esterna, la supervisione umana deve essere sempre garantita e documentabile.

9. GOVERNANCE, MONITORAGGIO E AGGIORNAMENTO

Il Responsabile del Servizio Digital Transformation, in raccordo con il Responsabile della Transizione Digitale (RTD), coordina l'adozione dell'intelligenza artificiale all'interno dell'Ente, sentito il Responsabile della Protezione dei Dati (DPO) per la verifica della conformità al GDPR (CAD art. 17, comma 1; GDPR art. 39).

In documenti specifici, legati ai singoli sistemi di Intelligenza Artificiale sviluppati, vengono definite responsabilità puntuali con riferimento ai seguenti aspetti:

- valutazione dei rischi e dell'affidabilità di un nuovo sistema;
- autorizzazione al deployment;
- monitoraggio delle prestazioni dei sistemi di IA nel tempo;
- gestione di eventuali incidenti;
- dismissione del sistema e gestione dei dati residui.

È attivata la casella di posta elettronica rtd@unioncamere.it quale canale dedicato per la segnalazione al RTD, da parte di dipendenti e collaboratori, di eventuali anomalie e situazioni critiche nell'utilizzo dei sistemi di IA. Tale canale non è destinato a quesiti di natura operativa o a dubbi applicativi. Il RTD assicura la trattazione tempestiva e la documentazione delle segnalazioni ricevute, coinvolgendo il DPO in presenza di implicazioni sui dati personali e il Segretario Generale nei casi di particolare gravità o di potenziale impatto significativo sui diritti fondamentali.

La Camera di Commercio definisce obiettivi monitorabili per la gestione dell'intelligenza artificiale, comunicati alle funzioni competenti e rivisti con cadenza almeno annuale. Gli obiettivi riguardano almeno:

- la formazione del personale: percentuale di dipendenti e collaboratori che utilizzano sistemi di IA adeguatamente formati;
- la completezza documentale: per ciascun sistema in uso, completamento delle valutazioni di impatto e di rischio previste dalla presente policy;
- la gestione degli incidenti: tempi di presa in carico e di risoluzione degli incidenti IA segnalati;
- la revisione periodica: rispetto delle scadenze di aggiornamento della presente policy, del Regolamento e delle procedure operative.



Per ciascun sistema di IA in uso, possono essere inoltre definiti indicatori specifici di prestazione relativi all'accuratezza, all'affidabilità e alla soddisfazione degli utilizzatori, documentati nel fascicolo del sistema.

I dirigenti vigilano sull'applicazione della presente policy all'interno delle rispettive strutture organizzative, promuovendo l'uso corretto dei sistemi di intelligenza artificiale e segnalando al **RTD** eventuali criticità operative o esigenze di aggiornamento.

La Camera di Commercio si impegna a effettuare:

- la tenuta e l'aggiornamento continuo di un Registro dei sistemi di intelligenza artificiale, che documenta per ciascun sistema almeno: denominazione e fornitore, descrizione e finalità, tipologia (generativa, predittiva, automazione, altro), classificazione di rischio ai sensi dell'AI Act, data di adozione, responsabile interno, stato (in valutazione / attivo / sospeso / dismesso), esito delle valutazioni di impatto e di rischio, data dell'ultima revisione. Per i sistemi ad alto rischio, il Registro assolve anche alla funzione di documentazione necessaria alla registrazione nella banca dati dell'UE di cui all'art. 49 dell'AI Act. Il Registro viene sottoposto a verifica complessiva almeno una volta l'anno;
- la revisione della policy con cadenza almeno annuale e, in ogni caso, in occasione di: modifiche normative significative (es. aggiornamento dell'AI Act, adozione di atti delegati o di esecuzione, evoluzione delle Linee Guida AgID), modifiche organizzative rilevanti, ovvero ogni qualvolta emergano elementi che ne rendano necessario l'aggiornamento.

La Camera di Commercio garantisce, inoltre, adeguata formazione al personale che utilizza sistemi di intelligenza artificiale, con particolare attenzione a:

- rischi di bias e discriminazione;
- limiti dei sistemi di IA;
- obblighi di riservatezza e protezione dei dati;
- responsabilità individuali.

La formazione è periodicamente aggiornata e documentata.

10.DOCUMENTI COLLEGATI

Le modalità operative per l'utilizzo di Sistemi di IA sono descritte nel "Disciplinare sull'uso dei sistemi di Intelligenza Artificiale".