INNOVAPUGLIA S.P.A.

Società in house della Regione Puglia

POLICY SULL'USO DELL'INTELLIGENZA ARTIFICIALE

Approvata con Determinazione del Direttore Generale n. 57 del 15 luglio 2026

INDICE

Art. 1 – Premesse e finalità

1.1 InnovaPuglia S.p.A. (di seguito "Società"), società in house della Regione Puglia e componente del Comitato Tecnico del Centro di competenza regionale sull'Intelligenza Artificiale nella Pubblica Amministrazione (D.G.R. n. 1488/2023), riconosce nell'intelligenza artificiale uno strumento strategico per il miglioramento dell'efficienza operativa, la qualità dei servizi e l'innovazione dei processi.

1.2 La presente Policy disciplina l'utilizzo dei sistemi di intelligenza artificiale da parte di tutto il personale della Società, nel rispetto del quadro normativo europeo e nazionale e dei principi etici di trasparenza, equità, sicurezza e responsabilità ivi inclusi il Regolamento (UE) 2024/1689, la Legge n. 132/2025, il GDPR e la normativa nazionale vigente e loro s.m.i.

1.3 La Policy persegue le seguenti finalità:

a) garantire un utilizzo responsabile, etico e conforme dell'IA;
b) tutelare i diritti fondamentali delle persone interessate;
c) proteggere i dati personali e le informazioni aziendali;
d) definire ruoli, responsabilità e procedure operative;
e) promuovere la consapevolezza e le competenze del personale in materia di IA.

Art. 2 – Riferimenti normativi

2.1 La presente Policy è adottata in conformità alle seguenti fonti normative:

a) Regolamento (UE) 2024/1689 del 13 giugno 2024 (AI Act);
b) Regolamento (UE) 2016/679 (GDPR) e D.Lgs. 196/2003 (Codice Privacy) come modificato dal D.Lgs. 101/2018;
c) Legge 23 settembre 2025, n. 132 – Disposizioni e deleghe al Governo in materia di intelligenza artificiale;
d) "Linee Guida per lo sviluppo di sistemi di Intelligenza Artificiale nella pubblica amministrazione" e le "Linee Guida per il procurement di IA nella Pubblica Amministrazione" adottate con la Determinazione n.43/2026 dell'Agenzia per l'Italia Digitale AGID;
e) Legge Regionale della Regione Puglia del 14 aprile 2025, n. 4 "Misure di promozione in materia di innovazione aperta e intelligenza artificiale e disposizioni varie".
f) Legge 28 giugno 2024 n. 90 - Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici;
g) Legge 22 aprile 1941, n. 633 – Legge sul diritto d'autore, come modificata dalla L. 132/2025;
h) Legge 20 maggio 1970, n. 300 – Statuto dei Lavoratori (art. 4);
i) D.Lgs. 7 marzo 2005, n. 82 – Codice dell'Amministrazione Digitale (CAD);
j) D.Lgs. 4 settembre 2024, n. 138 – Recepimento Direttiva NIS 2.

Art. 3 – Definizioni

3.1 Ai fini della presente Policy si intende per:

a) **Sistema di Intelligenza Artificiale (Sistema IA):** un sistema automatizzato progettato per operare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce, dagli input che riceve, come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali (art. 3, par. 1, AI Act);
b) **Provider (Fornitore):** soggetto che sviluppa o fa sviluppare un sistema di IA e lo immette sul mercato o lo mette in servizio con il proprio nome o marchio;
c) **Deployer (Operatore):** soggetto che utilizza un sistema di IA sotto la propria autorità, salvo nel caso in cui il sistema sia utilizzato nel corso di un'attività personale non professionale;
d) **IA Generativa:** sistema di IA capace di generare contenuti testuali, visivi, audio o multimediali sulla base di input (prompt) forniti dall'utente;
e) **AI Literacy:** insieme di competenze, conoscenze e comprensione che consentono ai soggetti interessati di effettuare un utilizzo informato dei sistemi di IA;
f) **FRIA (Fundamental Rights Impact Assessment):** valutazione d'impatto sui diritti fondamentali prevista per i sistemi di IA ad alto rischio;
g) **Referente IA:** figura interna designata dalla Società per il coordinamento delle attività in materia di intelligenza artificiale;
h) **Registro degli strumenti IA:** censimento interno di tutti i sistemi di intelligenza artificiale autorizzati all'uso nella Società.

Art. 4 – Ambito di applicazione

4.1 La presente Policy si applica a:

a) tutto il personale dipendente della Società, a qualsiasi livello e inquadramento;
b) i collaboratori esterni, i consulenti, i tirocinanti e i soggetti che a qualsiasi titolo operano per conto della Società;

c) gli amministratori e i componenti degli organi societari;
d) i fornitori e partner che trattano dati o erogano servizi utilizzando sistemi di IA per conto della Società.

4.2 La Policy si applica a tutti i sistemi di intelligenza artificiale:

e) acquisiti dalla Società e utilizzati internamente (es. Microsoft Copilot, chatbot, assistenti virtuali);
f) sviluppati internamente o commissionati dalla Società;
g) integrati in applicazioni o servizi erogati dalla Società;
h) utilizzati, anche gratuitamente, per finalità lavorative.

Art. 5 – Principi generali

5.1 L'utilizzo dei sistemi di IA nella Società è improntato ai seguenti principi:

5.1.1 Centralità della persona

L'IA è utilizzata come strumento al servizio dell'essere umano. Le decisioni che producono effetti giuridici o incidono significativamente sulle persone devono sempre prevedere una supervisione umana significativa.

5.1.2 Trasparenza

L'uso di sistemi di IA deve essere comunicato in modo chiaro ai soggetti interessati. I criteri e la logica sottostante al funzionamento dei sistemi devono essere comprensibili e accessibili.

5.1.3 Tracciabilità

L'utilizzo dei sistemi di IA deve essere documentato e ricostruibile, garantendo la conservazione dei log e delle informazioni necessarie a verificare il corretto funzionamento e le responsabilità.

5.1.4 Non discriminazione

I sistemi di IA non devono produrre output discriminatori per ragioni di sesso, razza, origine etnica, religione, disabilità, età, orientamento sessuale o qualsiasi altra condizione personale.

5.1.5 Sicurezza e affidabilità

I sistemi di IA devono essere sicuri, affidabili e robusti, progettati per minimizzare i rischi di errore, malfunzionamento o uso improprio.

5.1.6 Accountability

La responsabilità per l'utilizzo dei sistemi di IA e per gli output generati rimane sempre in capo alle persone fisiche e agli organi competenti, secondo le rispettive attribuzioni.

Art. 6 – Governance e figure di riferimento

6.1 La governance dell'IA nella Società è articolata come segue:

6.1.1 Direttore Generale

È responsabile dell'approvazione della presente Policy, dell'autorizzazione all'adozione di sistemi IA ad alto rischio e della vigilanza complessiva sull'attuazione delle disposizioni.

6.1.2 Referente IA

È designato dal Direttore Generale e svolge le seguenti funzioni:

- coordinamento delle attività in materia di IA;
- gestione del Registro degli strumenti IA;
- valutazione delle richieste di autorizzazione;
- supporto alla classificazione dei sistemi secondo l'AI Act;
- coordinamento con DPO, RTD e Ufficio ICT;
- promozione e monitoraggio delle attività formative;
- gestione delle segnalazioni e degli incidenti.

6.1.3 Data Protection Officer (DPO)

È coinvolto nelle valutazioni d'impatto (DPIA) e nelle verifiche di conformità al GDPR relative ai sistemi di IA che trattano dati personali.

6.1.4 Responsabile per la Transizione Digitale (RTD)

Collabora con il Referente IA per l'integrazione dei sistemi di IA nei processi di trasformazione digitale della Società e degli enti serviti.

6.1.5 Responsabili di Divisione/Settore

Sono responsabili dell'attuazione della Policy nelle rispettive strutture, della formazione del personale assegnato e della segnalazione di eventuali criticità.

Art. 7 – Registro degli strumenti di IA

7.1 È istituito il Registro degli strumenti di IA, tenuto e aggiornato dal Referente IA, contenente l'elenco di tutti i sistemi di intelligenza artificiale autorizzati all'uso nella Società.

7.2 Per ciascun sistema, il Registro riporta almeno le seguenti informazioni:

a) denominazione e versione del sistema;
b) fornitore e data di acquisizione/attivazione;
c) classificazione del rischio ai sensi dell'AI Act;
d) finalità e ambiti d'uso autorizzati;
e) categorie di dati trattati;
f) responsabile interno del sistema;
g) eventuali valutazioni d'impatto (FRIA, DPIA) effettuate;
h) data dell'ultima revisione.

7.3 È vietato l'utilizzo di sistemi di IA non inseriti nel Registro.

7.4 Il Registro è soggetto a revisione almeno annuale ed è pubblicato, per estratto, nella sezione "Amministrazione Trasparente" del sito istituzionale.

Art. 8 – Classificazione dei sistemi di IA

8.1 Ogni sistema di IA è classificato secondo i livelli di rischio previsti dall'AI Act:

LIVELLO	CARATTERISTICHE	ADEMPIMENTI
Minimo	Sistemi che non pongono rischi significativi	Inserimento nel Registro
Limitato	Sistemi che interagiscono con persone o generano contenuti	Registro + Obblighi di trasparenza + DPIA ove ne

LIVELLO	CARATTERISTICHE	ADEMPIMENTI
		ricorrano i presupposti ex art. 35 GDPR
Alto	Sistemi in ambiti sensibili (Allegato III AI Act)	Registro + FRIA + DPIA + Documentazione tecnica + Autorizzazione DG + registrazione **banca dati UE ex art. 49 AI Act per utilizzo di sistemi ad alto rischio.**
Di AI Inaccettabile	Sistemi vietati (art. 5 AI Act)	VIETATI – Nessun utilizzo consentito

8.2 La classificazione è effettuata dal Referente IA in collaborazione con il responsabile richiedente, tenendo conto sia della classificazione del fornitore sia dello specifico utilizzo previsto.

Art. 9 – Procedura di autorizzazione

9.1 L'introduzione di un nuovo sistema di IA o l'estensione dell'uso di un sistema esistente a nuove finalità richiede l'autorizzazione preventiva secondo la seguente procedura:

1. **Richiesta:** Il responsabile della struttura interessata presenta richiesta al Referente IA, descrivendo il sistema, le finalità, i dati trattati e gli utenti coinvolti.
2. **Classificazione:** Il Referente IA effettua la classificazione del rischio ai sensi dell'art. 8.
3. **Valutazioni:** Sono predisposte le valutazioni d'impatto richieste dalla classificazione (FRIA, DPIA), con il coinvolgimento del DPO. La FRIA, obbligatoria per i sistemi ad alto rischio ai sensi dell'art. 27 AI Act, comprende almeno: (a) descrizione dei processi in cui il sistema sarà utilizzato; (b) periodo e frequenza d'uso previsti; (c) categorie di persone fisiche e gruppi interessati; (d) rischi specifici di danno; (e) misure di sorveglianza umana; (f) misure da adottare in caso di concretizzazione dei rischi.
4. **Parere ICT:** Divisione ICT verifica la compatibilità tecnica e le misure di sicurezza.
5. **Verifica registrazione banca dati UE:** Per i sistemi ad alto rischio, prima della messa in servizio, il Referente IA verifica che il fornitore abbia registrato il sistema nella banca dati UE ex art. 49 AI Act. In mancanza di registrazione del sistema da parte del fornitore, il sistema non può essere utilizzato e il fornitore ne è informato (art. 26, par. 8, AI Act). Nel caso in cui il sistema, invece, sia stato già censito dal fornitore, Società, in qualità di deployer-autorità pubblica, provvede altresì alla registrazione del proprio uso del sistema ad alto rischio , nella banca dati UE (art. 49, par. 3, AI Act)
6. **Autorizzazione:** Il Referente IA autorizza i sistemi a rischio minimo/limitato; il Direttore Generale autorizza i sistemi ad alto rischio.
7. **Registrazione:** Il sistema autorizzato è inserito nel Registro.

9.2 Per i sistemi già in uso alla data di entrata in vigore della presente Policy, la procedura di cui al comma 1 è completata entro 180 giorni.

Art. 10 – Regole generali d'uso

10.1 Il personale autorizzato all'uso di sistemi di IA deve attenersi alle seguenti regole:

1. **Verifica degli output:** ogni output generato dall'IA deve essere verificato prima dell'utilizzo. L'utente è responsabile della correttezza e appropriatezza dei contenuti che utilizza.
2. **Supervisione umana:** l'IA è utilizzata come strumento di supporto, mai in sostituzione del giudizio umano per decisioni rilevanti.

3. **Finalità lavorative:** l'uso dei sistemi di IA aziendali è consentito esclusivamente per finalità lavorative.
4. **Riservatezza:** è vietato inserire nei sistemi di IA informazioni riservate, dati personali sensibili o segreti aziendali, salvo che il sistema sia espressamente autorizzato per tale trattamento.
5. **Documentazione:** per procedimenti amministrativi rilevanti, l'utilizzo di sistemi di IA deve essere documentato.
6. **Segnalazione:** eventuali malfunzionamenti, output problematici o dubbi sull'appropriatezza dell'uso devono essere tempestivamente segnalati al Referente IA.

7. **Informazione preventiva ai lavoratori:** prima di mettere in servizio o utilizzare un sistema di IA ad alto rischio sul luogo di lavoro, i Responsabili di Divisione/Settore interessati informano i lavoratori e i loro rappresentanti che saranno soggetti all'uso del sistema (art. 26, par. 7, AI Act e art. 11, comma 2, L. 132/2025).

Art. 11 – Divieti

11.1 È fatto assoluto divieto di:

1. utilizzare sistemi di IA non inseriti nel Registro o non autorizzati;
2. utilizzare sistemi di IA vietati ai sensi dell'art. 5 dell'AI Act (utilizzare sistemi di IA che integrano le pratiche vietate dall'art. 5, par. 1, AI Act: tecniche manipolative subliminali (lett. a); sfruttamento di vulnerabilità (lett. b); social scoring (lett. c); valutazione del rischio di reato basata solo su profilazione (lett. d); scraping facciale non mirato (lett. e); riconoscimento delle emozioni sul lavoro e a scuola (lett. f); categorizzazione biometrica per dati sensibili (lett. g); identificazione biometrica remota in tempo reale in spazi pubblici (lett. h).adottare decisioni automatizzate che producono effetti giuridici su persone fisiche senza supervisione umana;
3. utilizzare l'IA per attività di profilazione di dipendenti o utenti senza autorizzazione;
4. inserire nei sistemi di IA categorie particolari di dati personali (art. 9 GDPR) o dati giudiziari (art. 10 GDPR) senza autorizzazione specifica;
5. generare contenuti falsi, ingannevoli, discriminatori, diffamatori o lesivi della dignità delle persone;
6. tentare di aggirare le misure di sicurezza o i filtri dei sistemi (jailbreak, prompt injection);
7. utilizzare l'IA per il controllo a distanza dell'attività dei lavoratori in violazione dell'art. 4 dello Statuto dei Lavoratori;
8. condividere credenziali di accesso ai sistemi di IA o utilizzare credenziali altrui.

Art. 12 – Obblighi di trasparenza e tracciabilità

12.1 Ai sensi dell'art. 14 della L. 132/2025 e dei principi di trasparenza e tracciabilità previsti dalla normativa europea e nazionale applicabile, la Società assicura la conoscibilità del funzionamento e la tracciabilità dell'utilizzo dei sistemi di IA.

12.2 Obblighi di trasparenza verso gli utenti esterni:

- quando un utente interagisce con un sistema di IA (chatbot, assistente virtuale), deve essere chiaramente informato che sta interagendo con un sistema automatizzato;
- i contenuti generati o manipolati dall'IA (deepfake, testi sintetici) devono essere identificati come tali;
- deve essere garantita la possibilità di richiedere l'intervento di un operatore umano.

12.3 Obblighi di trasparenza nei documenti ufficiali:

Qualora la Società pubblichi testi generati o manipolati da sistemi di IA allo scopo di informare il pubblico su questioni di interesse pubblico, è reso noto che il testo è stato generato o

manipolato artificialmente . Tale obbligo non si applica se il contenuto è stato sottoposto a un processo di revisione umana o di controllo editoriale e una persona fisica o giuridica detiene la responsabilità editoriale della pubblicazione del contenuto (art. 50, par. 4, AI Act). 12.4 La Società conserva i log di utilizzo dei sistemi di IA per il tempo necessario a garantire la tracciabilità. Per i sistemi ad alto rischio, il periodo di conservazione non è inferiore a sei mesi, ai sensi dell'art. 26, par. 6, AI Act. Per tutti i sistemi, la conservazione è comunque garantita per un periodo non inferiore a quello di conservazione degli atti amministrativi cui i log si riferiscono

Art. 13 – Protezione dei dati personali

13.1 L'utilizzo di sistemi di IA che trattano dati personali deve rispettare integralmente il GDPR e il Codice Privacy.

13.2 In particolare:

1. il Registro dei trattamenti (art. 30 GDPR) è aggiornato per includere i trattamenti effettuati mediante sistemi di IA;
2. le informative agli interessati (artt. 13-14 GDPR) sono integrate con le informazioni relative all'uso dell'IA, inclusa la logica sottostante;
3. per i sistemi ad alto rischio o che trattano dati su larga scala è effettuata la DPIA (art. 35 GDPR);
4. sono rispettati i principi di minimizzazione dei dati, limitazione delle finalità e limitazione della conservazione;
5. i fornitori di sistemi di IA che trattano dati personali per conto della Società sono designati responsabili del trattamento ai sensi dell'art. 28 GDPR.

13.3 Microsoft, fornitore di Copilot, ha dichiarato che i dati aziendali (prompt e risposte) non sono utilizzati per l'addestramento dei modelli di base.

La garanzia deve essere verificata contrattualmente per ogni fornitore di sistemi di IA.

Art. 14 – Proprietà intellettuale e diritto d'autore

14.1 L'utilizzo di sistemi di IA generativa deve rispettare la normativa sul diritto d'autore (L. 633/1941, come modificata dalla L. 132/2025).

14.2 In particolare:

1. è vietato utilizzare contenuti protetti da diritto d'autore come input per sistemi di IA senza le necessarie autorizzazioni;
2. i contenuti generati dall'IA che incorporano elementi creativi originali possono essere tutelati come opere dell'ingegno solo se è presente un apporto creativo umano significativo;
3. l'utilizzo di output generati dall'IA deve essere verificato per escludere violazioni di diritti di terzi;
4. la Società mantiene la titolarità degli output generati dai propri dipendenti nell'ambito dell'attività lavorativa.

Art. 15 – Sicurezza informatica

15.1 I sistemi di IA sono integrati nel framework di sicurezza informatica della Società, in conformità al D.Lgs. 138/2024 (NIS2) e alla L. 90/2024.

15.2 Le misure di sicurezza includono:

1. autenticazione forte per l'accesso ai sistemi di IA;

2. cifratura dei dati in transito e a riposo;
3. protezione contro attacchi specifici (prompt injection, jailbreak, data poisoning);
4. monitoraggio delle anomalie e degli accessi;
5. backup e procedure di disaster recovery;
6. test periodici di vulnerabilità e penetration testing.

Art. 16 – Formazione e AI Literacy

16.1 In attuazione dell'art. 4 dell'AI Act ed in coerenza con gli obblighi di alfabetizzazione in materia di IA previsti dall'AI Act, la Società promuove programmi di AI Literacy per tutto il personale.

16.2 La formazione comprende:

1. **Formazione base (obbligatoria per tutti):** principi generali, quadro normativo, regole d'uso, rischi e opportunità;
2. **Formazione avanzata (per utilizzatori intensivi):** funzionamento dei modelli, prompt engineering, valutazione critica degli output;
3. **Formazione specialistica (per sviluppatori e referenti):** classificazione dei rischi, valutazioni d'impatto, compliance, sicurezza.

16.3 Il completamento della formazione base è requisito per l'abilitazione all'uso dei sistemi di IA.

16.4 Le attività formative sono finanziate con le risorse disponibili, incluse le economie PNRR ai sensi della Direttiva DTD del 23 gennaio 2025.

Art. 17 – Monitoraggio e audit

17.1 Il Referente IA, in collaborazione con le strutture competenti, effettua il monitoraggio continuo dell'utilizzo dei sistemi di IA.

17.2 Sono previsti:

1. **Monitoraggio operativo:** verifica del corretto funzionamento, delle prestazioni e dell'accuratezza degli output;
2. **Audit di conformità:** verifica periodica (almeno annuale) del rispetto della presente Policy, dell'AI Act e della L. 132/2025;
3. **Test di bias:** verifica periodica dell'assenza di discriminazioni negli output;
4. **Revisione del Registro:** aggiornamento annuale del Registro degli strumenti IA.

17.3 Gli esiti degli audit sono documentati e comunicati al Direttore Generale. Le criticità rilevate sono oggetto di piani di remediation.

Art. 18 – Segnalazioni e gestione degli incidenti

18.1 Il personale è tenuto a segnalare tempestivamente al Referente IA:

- output manifestamente errati, inappropriati o potenzialmente discriminatori;
- malfunzionamenti o comportamenti anomali dei sistemi;
- tentativi di accesso non autorizzato o violazioni della sicurezza;
- utilizzi impropri da parte di altri soggetti;
- dubbi sull'appropriatezza di un determinato utilizzo.

18.2 Le segnalazioni possono essere effettuate via email al Referente IA o attraverso i canali di whistleblowing aziendale.

18.3 In caso di incidenti gravi che comportino rischi per i diritti fondamentali o violazioni di dati personali, si applicano le procedure di notifica previste dall'AI Act (art. 73) e dal GDPR (artt.

33-34). Il Referente IA, qualora abbia individuato un incidente grave, ne informa immediatamente il fornitore, in primo luogo, e successivamente le pertinenti autorità di vigilanza del mercato. Per l'Italia, l'autorità di vigilanza del mercato è l'ACN, designata quale Autorità nazionale per l'IA ai sensi dell'art. 20 L. 132/2025 (art. 26, par. 5, AI Act). Se non è possibile raggiungere il fornitore, si applica mutatis mutandis l'art. 73 AI Act.

Art. 19 – Responsabilità e regime sanzionatorio

19.1 La violazione della presente Policy costituisce illecito disciplinare ai sensi del CCNL applicabile e può comportare l'applicazione delle sanzioni previste, proporzionate alla gravità della violazione.

19.2 Fermo restando quanto previsto dal comma 1, la violazione può altresì comportare:

- responsabilità civile per i danni cagionati alla Società o a terzi;
- responsabilità penale per le fattispecie di reato previste dalla L. 132/2025 e dal Codice penale;
- responsabilità amministrativa della Società ai sensi del D.Lgs. 231/2001.

19.3 Il Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001 è aggiornato per includere i rischi-reato connessi all'uso dell'intelligenza artificiale.

Art. 20 – Disposizioni finali

20.1 La presente Policy entra in vigore dalla data di approvazione ed è pubblicata:

- nella intranet aziendale;
- nella sezione "Amministrazione Trasparente – Uso dell'intelligenza artificiale" del sito istituzionale;
- ed è comunicata a tutto il personale.

20.2 La Policy è soggetta a revisione almeno annuale o in occasione di:

- modifiche significative del quadro normativo;
- introduzione di nuovi sistemi di IA;
- esiti di audit che evidenzino criticità;
- emanazione di nuove linee guida AgID o ACN, nonché dell’adozione o aggiornamento di linee guida AgID e di eventuali provvedimenti delle Autorità nazionali competenti”

20.3 Per quanto non espressamente previsto dalla presente Policy, si rinvia alla normativa vigente e alle disposizioni aziendali in materia di protezione dei dati personali, sicurezza informatica e condotta del personale e dai provvedimenti attuativi, regolatori e di coordinamento nazionale adottati o da adottarsi dalle autorità competenti, ivi inclusi quelli relativi alla governance, vigilanza, notifica, coordinamento interistituzionale e applicazione operativa della normativa in materia di intelligenza artificiale

Il Direttore Generale
Ing. Francesco Surico

ALLEGATI

Allegato A – Modulo di richiesta autorizzazione sistema IA
Allegato B – Template Registro degli strumenti IA
Allegato C – Template FRIA (Fundamental Rights Impact Assessment)
Allegato D – Guida operativa per i dipendenti
Allegato E – Elenco sistemi IA autorizzati (estratto del Registro)