# REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI DI INTELLIGENZA ARTIFICIALE

| | |
|---|---|
| **Versione:** | 1.0 |
| **Anno:** | 2026 |
| **Approvazione** | Comitato di Indirizzo – deliberazione n. 19 del 12 maggio 2026 |

# Sommario

## GLOSSARIO

**Intelligenza Artificiale (IA):** sistema basato su tecniche informatiche avanzate progettato per operare con diversi livelli di autonomia e che può presentare capacità di adattamento dopo la messa in funzione, in grado di dedurre, per obiettivi espliciti o impliciti, come generare risultati quali contenuti, previsioni, raccomandazioni o decisioni che influenzano ambienti fisici o virtuali (definizione ex Regolamento (UE) 2024/1689 — AI Act).

**IA generativa:** sistema di intelligenza artificiale in grado di generare testo, immagini, audio, video o altri contenuti in risposta a istruzioni (prompt) fornite dall'utente.

**Prompt:** istruzione o richiesta fornita a un sistema di IA generativa per ottenere un risultato specifico. Il prompt può contenere testo, domande o indicazioni operative.

**Supervisione umana:** processo mediante il quale una persona competente verifica, valida e, se necessario, corregge o integra i contenuti prodotti da un sistema di IA, prima del loro utilizzo o diffusione.

**Logging:** registrazione automatica delle operazioni svolte su un sistema informatico, al fine di garantirne la tracciabilità e la possibilità di verifica successiva.

**Bias:** distorsione sistematica presente nei dati o negli algoritmi che può condurre a risultati discriminatori o non equi.

**Sistema ad alto rischio:** sistema di IA che, per le sue caratteristiche e ambiti di utilizzo, può avere un impatto significativo sui diritti fondamentali delle persone o sulla sicurezza, come definito dall'AI Act.

**Referente AI:** funzionario informatico designato che coordina l'applicazione delle disposizioni del presente Regolamento e supporta il Direttore e il RTD nella predisposizione delle regole tecniche operative.

**RTD — Responsabile per la Transizione Digitale:** figura prevista dall'art. 17 del D.Lgs. 82/2005 (CAD), responsabile della governance complessiva dei sistemi informativi e dell'adozione degli strumenti di IA.

**Whitelist:** elenco degli strumenti di IA generativa approvati per l'utilizzo nell'ambito lavorativo, aggiornato periodicamente dal Referente AI su indicazione del RTD.

**DPO — Data Protection Officer:** responsabile della protezione dei dati personali ai sensi del Reg. (UE) 2016/679 (GDPR).

**DPIA:** Valutazione d'Impatto sulla Protezione dei Dati (art. 35 GDPR), obbligatoria quando il trattamento può presentare rischi elevati per i diritti e le libertà delle persone fisiche.

**FRIA:** Valutazione d'Impatto sui Diritti Fondamentali (art. 27 AI Act), obbligatoria per i sistemi di IA ad alto rischio.

**Deployer (utilizzatore):** soggetto pubblico o privato che utilizza un sistema di IA sotto la propria autorità, ad eccezione di usi puramente personali e non professionali (definizione ex art. 3, n. 4, Regolamento (UE) 2024/1689 — AI Act). AIPo si qualifica, in via ordinaria, come deployer.

**Registro dei sistemi di IA:** inventario interno dei sistemi di Intelligenza Artificiale adottati dall'Agenzia, con indicazione di finalità, fornitore, classificazione di rischio, unità organizzativa titolare, esito di DPIA e FRIA.

**Deepfake:** contenuto sintetico (immagine, audio, video o testo) generato o manipolato con tecniche di IA in modo da apparire autentico e potenzialmente idoneo a trarre in inganno il destinatario, soggetto a obblighi di etichettatura ai sensi dell'art. 50 del Regolamento (UE) 2024/1689 (AI Act).

## QUADRO NORMATIVO DI RIFERIMENTO

Il presente Regolamento è redatto e aggiornato nel rispetto del seguente quadro normativo e regolatorio (come modificato e integrato nel tempo). Restano fermi gli ulteriori obblighi settoriali eventualmente applicabili.

**A) Normativa dell'Unione Europea**

- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (GDPR).
- Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 (c.d. "NIS2").
- Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 (c.d. "AI Act").

**B) Normativa nazionale**

- Legge 28 giugno 2024, n. 90, recante disposizioni in materia di rafforzamento della cybersicurezza nazionale e resilienza delle pubbliche amministrazioni.
- Decreto legislativo 4 settembre 2024, n. 138, di recepimento della Direttiva (UE) 2022/2555 (NIS2).
- Legge 23 settembre 2025, n. 132, recante "Disposizioni e deleghe al Governo in materia di intelligenza artificiale".
- Decreto legislativo 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale — CAD) e s.m.i.
- Decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) e s.m.i.
- Decreto legislativo 152/2006 (Codice dell'Ambiente).
- Direttiva 2000/60/CE (Direttiva Quadro Acque).

**C) Linee guida e atti di indirizzo**

- Linee guida per l'adozione di IA nella pubblica amministrazione, emanate dall'Agenzia per l'Italia Digitale (AgID) ai sensi del D.P.C.M. 12 gennaio 2024 (versione 1.0 del 14 febbraio 2025).
- Standard ISO/IEC 42001:2023 "Information technology — Artificial intelligence — Management system".
- Linee guida per uno sviluppo sicuro dell'Intelligenza Artificiale (National Cyber Security Centre del Regno Unito, 27 novembre 2023, sottoscritte da ACN).
- Determinazione AgID n. 43 del 10 marzo 2026, recante le linee guida per lo sviluppo e l'approvvigionamento di sistemi di Intelligenza Artificiale da parte delle Pubbliche Amministrazioni.
- Linee guida ACN per la sicurezza delle banche dati della Pubblica Amministrazione (novembre 2024) e indicazioni operative dell'Agenzia per la Cybersicurezza Nazionale in materia di resilienza e gestione degli incidenti.

**D) Documentazione interna di riferimento**

- Documento di governance della sicurezza informatica e gestione del rischio ICT di AIPo.
- Regolamento per l'utilizzo degli strumenti informatici di AIPo.
- Manuale di segnalazione e gestione degli incidenti informatici di AIPo.
- Circolare informativa sul Referente per la cybersicurezza (Prot. 483 del 9 gennaio 2025).

## ART. 1 — FINALITÀ E AMBITO DI APPLICAZIONE

1. Il presente Regolamento disciplina le modalità di utilizzo degli strumenti di Intelligenza Artificiale generativa e, in quanto applicabile, dei sistemi di IA a finalità istituzionale adottati dall'Agenzia Interregionale per il fiume Po (AIPo), al fine di garantirne un impiego responsabile e conforme alla normativa vigente, tenendo conto dei rischi potenziali connessi alla riservatezza delle informazioni, alla protezione dei dati personali, alla sicurezza dei sistemi informativi e alla tutela dei dati ambientali e idrografici.

2. Il Regolamento si inserisce nel quadro complessivo della governance della sicurezza informatica di AIPo e si coordina con:

a) il Regolamento per l'utilizzo degli strumenti informatici, che definisce le regole generali per l'uso delle risorse ICT;

b) il Documento di governance della sicurezza informatica e gestione del rischio ICT, che disciplina le politiche e le misure organizzative per la tutela dei sistemi informativi;

c) il Manuale di segnalazione e gestione degli incidenti informatici, che definisce le procedure per la gestione di eventi che possano compromettere la sicurezza dei sistemi.

3. Le disposizioni di cui al presente Regolamento si applicano a tutto il personale comunque denominato, inclusi dipendenti, collaboratori e consulenti esterni, nell'ambito dell'utilizzo degli strumenti di IA generativa per finalità lavorative.

4. Resta escluso dall'applicazione del presente Regolamento l'uso personale, al di fuori dell'ambito lavorativo, che comunque non deve interferire con il servizio né comportare l'impiego improprio delle risorse dell'Agenzia (rete, postazione, credenziali istituzionali).

5. Ai fini del presente Regolamento, l'Agenzia si qualifica come "deployer" (utilizzatore) di sistemi di Intelligenza Artificiale ai sensi dell'art. 3, n. 4, del Regolamento (UE) 2024/1689 (AI Act). Le disposizioni del Regolamento si applicano, in quanto compatibili, anche ai sistemi di IA non generativa e ai componenti di IA integrati (embedded) in software gestionali, applicativi di analisi dati o soluzioni di automazione documentale adottati da AIPo, con particolare riferimento a strumenti di elaborazione predittiva, di analisi di immagini da drone o satellitari e di supporto decisionale in ambito idraulico, idrologico e ambientale. Eventuali integrazioni e sviluppi software commissionati alle società in house sono soggetti ai medesimi presìdi di governance, trasparenza, sicurezza e documentazione previsti dal presente Regolamento.

## ART. 2 — PRINCIPI GENERALI

1. L'Agenzia riconosce l'opportunità rappresentata dall'introduzione degli strumenti di Intelligenza Artificiale generativa nelle attività lavorative per il miglioramento dell'efficienza, della qualità e della tempestività dei processi, nonché l'esigenza del loro utilizzo conformemente alle esigenze di tutela dei dati, trasparenza e accountability amministrativa.

2. L'impiego degli strumenti di Intelligenza Artificiale generativa avviene nel rispetto dei seguenti principi fondamentali:

- Responsabilità: il personale rimane pienamente responsabile dei contenuti prodotti con il supporto dell'IA, anche nel caso in cui questi siano generati automaticamente.
- Verifica umana e supervisione: ogni contenuto generato deve essere attentamente esaminato, validato e, se necessario, integrato o corretto, prima di essere utilizzato, diffuso o condiviso in contesti istituzionali o pubblici. Nessuna attività può essere delegata integralmente a un sistema automatizzato senza controllo umano. Particolare attenzione deve essere prestata alla verifica dei dati ambientali e idrografici generati o elaborati con supporto dell'IA.
- Trasparenza e spiegabilità: ove rilevante, è fatto obbligo di dichiarare l'impiego di strumenti di IA nella produzione di documenti, comunicazioni o analisi, in conformità alle disposizioni di cui alla Legge 23 settembre 2025, n. 132 e alle Linee guida AgID.

- Imparzialità e non discriminazione: è vietato l'utilizzo dell'IA generativa per produrre contenuti manipolativi, discriminatori, offensivi o contrari ai principi di imparzialità, equità e inclusione che ispirano l'azione dell'Agenzia.
- Sicurezza e protezione dei dati: non devono essere inseriti nei prompt informazioni personali, sensibili o riservate, dati ambientali non pubblici, dati di monitoraggio in corso di validazione, né documenti interni non pubblici.
- Tracciabilità e logging: gli strumenti di IA generativa utilizzati devono essere dotati di adeguati meccanismi di registrazione delle operazioni svolte, in conformità alle Linee guida AgID, al fine di garantire verificabilità e accountability.
- Trasparenza verso l'esterno: i contenuti sintetici (testi, immagini, audio, video) destinati a comunicazione pubblica o istituzionale, generati con il contributo determinante di sistemi di IA, sono etichettati in conformità all'art. 50 del Regolamento (UE) 2024/1689 (AI Act) e agli obblighi di cui alla Legge 23 settembre 2025, n. 132, al fine di consentire al destinatario di identificarne la natura artificiale.
- Tutela dei diritti degli interessati: nessuna decisione produttiva di effetti giuridici o comunque significativi nei confronti di cittadini, imprese o personale dell'Agenzia può essere basata unicamente su un trattamento automatizzato ai sensi dell'art. 22 del Regolamento (UE) 2016/679 (GDPR); è in ogni caso assicurato l'intervento umano significativo da parte di personale competente.
- Sostenibilità ambientale: nella selezione e nell'uso degli strumenti di IA si tiene conto, ove disponibili, degli indicatori di consumo energetico e di impatto ambientale dichiarati dal fornitore, privilegiando soluzioni proporzionate rispetto all'effettiva esigenza operativa ed evitando usi ridondanti o non necessari, in coerenza con la missione ambientale dell'Agenzia.

## ART. 3 — UTILIZZI CONSENTITI

1. L'utilizzo degli strumenti di Intelligenza Artificiale generativa per finalità lavorative è consentito esclusivamente se effettuato attraverso le dotazioni aziendali (hardware, software, credenziali e account istituzionali) e all'interno di ambienti informatici sicuri, nel rispetto delle policy dell'Agenzia e previa autorizzazione del Referente AI. L'autorizzazione avviene mediante l'inserimento dello strumento nella whitelist degli strumenti IA approvati, aggiornata dal Referente AI su indicazione del RTD con cadenza almeno semestrale, previa verifica della conformità al GDPR (inclusa la stipula del Data Processing Agreement ove richiesto), dell'adeguatezza delle misure di sicurezza del fornitore e della classificazione di rischio ai sensi dell'AI Act.

2. La whitelist è pubblicata nel portale intranet dell'Agenzia ed è comunicata a tutto il personale interessato. La responsabilità della governance degli strumenti IA è affidata al Direttore dell'Agenzia, con delega operativa al RTD, che ne risponde agli organi di vertice.

3. L'uso su dispositivi personali o tramite strumenti non approvati non è ammesso per attività lavorative, salvo diversa disposizione espressamente comunicata.

4. L'adozione di strumenti di IA generativa è ammessa solo per attività di supporto operativo e non può in alcun caso sostituire la responsabilità individuale nei processi decisionali. In particolare, l'uso è consentito per:

- redazione di bozze di testi, e-mail, report o documenti informativi, da sottoporre in ogni caso a verifica e validazione umana prima della diffusione o dell'utilizzo ufficiale;
- sintesi di documenti pubblici, raccolta di spunti per attività di analisi preliminare, supporto alla generazione di contenuti in fase di brainstorming;
- traduzioni automatiche, revisione ortografica e grammaticale, semplificazioni linguistiche e riformulazione di testi per finalità comunicative o divulgative;
- supporto nell'elaborazione di comunicazioni istituzionali destinate alle Regioni, agli enti locali e agli stakeholder, sempre previa verifica e validazione del contenuto.

5. L'approvvigionamento di strumenti e servizi di IA presso fornitori terzi, ivi comprese le società in house eventualmente incaricate di integrazioni o sviluppi, è subordinato all'inserimento nei relativi contratti, anche

mediante apposito addendum, delle seguenti clausole minime, coerenti con la Determinazione AgID n. 43 del 10 marzo 2026 e con il Regolamento (UE) 2024/1689 (AI Act):

- a) auditabilità del sistema di IA e diritto dell'Agenzia di richiedere informazioni tecniche e documentazione sul funzionamento, sui dataset di addestramento (ove pertinenti) e sulle metriche di performance e accuratezza;
- b) divieto di riuso dei dati, dei prompt e degli output dell'Agenzia per l'addestramento, il fine-tuning o il miglioramento dei modelli del fornitore, salvo espresso consenso scritto e specifico;
- c) residenza dei dati e localizzazione dei trattamenti nell'ambito dell'Unione Europea, con indicazione esplicita dei soggetti ultra-UE eventualmente coinvolti e delle relative garanzie ai sensi del Capo V del GDPR;
- d) messa a disposizione della documentazione tecnica di cui all'Allegato IV dell'AI Act per i sistemi classificati ad alto rischio, nonché delle istruzioni d'uso e delle informazioni rilevanti per la Valutazione d'Impatto sui Diritti Fondamentali (FRIA);
- e) SLA su disponibilità del servizio, tempi di intervento, gestione delle vulnerabilità di sicurezza, notifica tempestiva di incidenti e di eventuali comportamenti anomali, inclusi fenomeni di bias, drift o degrado delle performance;
- f) piano di uscita e fine-vita, con obbligo di restituzione o cancellazione certificata dei dati dell'Agenzia e di garantire la continuità operativa in caso di cessazione del servizio.

## ART. 4 — UTILIZZI VIETATI

1. È vietato l'utilizzo degli strumenti di Intelligenza Artificiale generativa in tutti i casi in cui l'attività possa comportare rischi per la riservatezza dei dati, la correttezza dell'azione amministrativa, l'integrità delle funzioni istituzionali dell'Agenzia o l'affidabilità dei dati ambientali e idrografici. In particolare, non è ammesso l'utilizzo dell'IA generativa per:

- inserire nei prompt dati personali, dati sensibili o giudiziari, informazioni protette da obblighi di segretezza, codici di accesso, credenziali, documenti interni non pubblici, dati ambientali non validati o in corso di elaborazione, dati di monitoraggio idrografico riservati;
- sostituire l'intervento umano nei processi decisionali discrezionali, in particolare per quanto riguarda l'esercizio di funzioni di pianificazione, valutazioni istruttorie, attività di vigilanza, monitoraggio ambientale, accertamenti ispettivi, valutazioni tecniche su opere idrauliche;
- elaborare, validare o certificare autonomamente dati ambientali, idrografici, idrologici, pluviometrici o relativi al monitoraggio del bacino del Po destinati a utilizzi ufficiali, reportistica istituzionale o trasmissione a enti terzi;
- simulare identità o generare contenuti ingannevoli, fuorvianti o non chiaramente attribuibili alla persona o struttura che li utilizza;
- utilizzare strumenti di IA generativa per scopi extraprofessionali durante l'orario di lavoro, in modo non occasionale o non autorizzato.
- produrre o diffondere, sui canali istituzionali o in comunicazioni riconducibili all'Agenzia, contenuti sintetici (immagini, audio, video o testi) di tipo "deepfake" o comunque generati artificialmente che non siano chiaramente etichettati come tali, ai sensi dell'art. 50 del Regolamento (UE) 2024/1689 (AI Act) e della Legge 23 settembre 2025, n. 132;
- ricorrere a pratiche di Intelligenza Artificiale vietate dall'art. 5 del Regolamento (UE) 2024/1689 (AI Act), ivi comprese tecniche manipolative o sfruttanti le vulnerabilità delle persone, il social scoring, il riconoscimento delle emozioni in ambito lavorativo (salve le eccezioni di legge) e la categorizzazione biometrica basata su caratteristiche sensibili.

2. La tabella riportata nell'Allegato 1 al presente Regolamento fornisce un insieme di casistiche esemplificative circa l'ammissibilità o non ammissibilità dell'utilizzo degli strumenti di IA nello svolgimento dell'attività lavorativa.

3. In caso di dubbi sull'ammissibilità di specifici utilizzi, è necessario consultare il Referente AI, che potrà coinvolgere il DPO per i profili inerenti alla protezione dei dati personali.

## ART. 5 — FORMAZIONE E SENSIBILIZZAZIONE

1. La formazione rappresenta il presupposto per garantire un utilizzo consapevole, sicuro e coerente degli strumenti di IA generativa all'interno dell'Agenzia.

2. L'utilizzo degli strumenti di Intelligenza Artificiale generativa è subordinato al completamento di un percorso formativo obbligatorio, secondo quanto previsto nel Piano di formazione dell'Agenzia e in conformità alle Linee guida AgID. In particolare:

- tutto il personale è tenuto a frequentare i moduli formativi disponibili sulla piattaforma nazionale Syllabus.gov.it, con particolare riferimento al percorso "Competenze emergenti" e ai moduli dedicati all'uso responsabile dell'IA nella Pubblica Amministrazione;
- in fase di prima attuazione, per poter accedere e utilizzare strumenti di IA generativa nell'ambito delle attività lavorative, è necessario aver completato almeno il livello intermedio del percorso formativo disponibile su Syllabus;
- il completamento del percorso formativo deve essere attestato mediante la piattaforma stessa o con altra documentazione valida, da trasmettere al Referente AI e all'Ufficio del Personale.
- in attuazione dell'obbligo di alfabetizzazione in materia di IA ("AI literacy") di cui all'art. 4 del Regolamento (UE) 2024/1689 (AI Act), applicabile dal 2 febbraio 2025, è assicurata una formazione ricorrente, con cadenza almeno annuale finalizzata a garantire un livello adeguato di competenze sull'utilizzo responsabile e consapevole dei sistemi di IA.

3. Il Referente AI, in raccordo con il RTD, promuove iniziative di formazione continua volte ad assicurare la comprensione dei principi di qualità dei dati, affidabilità e robustezza dei sistemi di IA, in conformità ai requisiti definiti dalle Linee guida AgID.

## ART. 6 — SEGNALAZIONE DI ANOMALIE E INCIDENTI

1. Qualsiasi anomalia, malfunzionamento o evento sospetto rilevato nell'utilizzo di strumenti di IA generativa deve essere tempestivamente segnalato secondo le modalità previste dal Manuale di segnalazione e gestione degli incidenti informatici dell'Agenzia.

2. Costituiscono situazioni che richiedono immediata segnalazione, in particolare:

- la generazione di contenuti manifestamente errati, incoerenti o potenzialmente dannosi;
- il sospetto di utilizzo improprio di strumenti di IA da parte di terzi o attraverso account compromessi;
- la divulgazione accidentale di informazioni riservate o dati personali attraverso prompt o interazioni con sistemi di IA;
- comportamenti anomali o inattesi degli strumenti di IA che possano indicare vulnerabilità di sicurezza.

3. La segnalazione deve essere effettuata tempestivamente al Referente AI e al Referente per la cybersicurezza, attraverso i canali indicati nel Manuale di gestione degli incidenti informatici. Qualora l'evento rientri nelle fattispecie di incidente significativo ai sensi del D.Lgs. 4 settembre 2024, n. 138 (NIS2), il Referente per la cybersicurezza attiva le procedure di notifica ad ACN nei termini di legge. Ove l'evento integri una violazione di dati personali, si applicano le procedure di notifica al Garante ai sensi dell'art. 33 GDPR, con coinvolgimento del DPO.

4. La mancata segnalazione di eventi o anomalie significative può comportare responsabilità disciplinari ai sensi del Codice di comportamento dell'Ente.

## ART. 7 — GOVERNANCE, MONITORAGGIO E RESPONSABILITÀ

1. La governance dell'utilizzo degli strumenti di IA è strutturata su tre livelli distinti e complementari, nel rispetto delle competenze di ciascuna figura:

| | |
|---|---|
| **COMITATO DI INDIRIZZO** | Responsabile della governance complessiva dell'IA in AIPo. Approva il Regolamento e i suoi aggiornamenti. Indirizza le scelte strategiche in materia di adozione degli strumenti di IA. |
| **RTD** | Responsabile per la Transizione Digitale (art. 17 CAD). Sovrintende alla governance tecnica degli strumenti di IA, assicura la conformità alle Linee guida AgID e risponde al Comitato di Indirizzo. Assegna le funzioni operative al Referente AI. |
| **REFERENTE AI** | Funzionario informatico designato. Coordina l'applicazione operativa del Regolamento, gestisce la whitelist, supporta Comitato di Indirizzo ed RTD nella predisposizione delle regole tecniche e delle disposizioni attuative, è il punto di riferimento per il personale. |

2. Il Referente AI, funzionario informatico designato, svolge in particolare le seguenti funzioni:

- coordina l'applicazione delle disposizioni del presente Regolamento e delle regole tecniche operative;
- gestisce e aggiorna la whitelist degli strumenti IA approvati, su indicazione del RTD;
- supporta il Comitato di Indirizzo e il RTD nella predisposizione e nell'aggiornamento delle regole tecniche attuative del Regolamento;
- costituisce il punto di riferimento del personale per dubbi interpretativi e operativi sull'utilizzo degli strumenti IA;
- coordina le attività di monitoraggio dell'utilizzo degli strumenti IA, in raccordo con il Referente per la cybersicurezza;
- promuove le iniziative di formazione e sensibilizzazione del personale.

3. L'utilizzo degli strumenti IA è soggetto a monitoraggio e verifiche periodiche da parte del Referente AI, in raccordo con il RTD e con il DPO per i profili di riservatezza e privacy.

4. Prima dell'adozione di qualsiasi strumento IA per finalità istituzionali, il Referente AI, in raccordo con il DPO, verifica la necessità di effettuare una Valutazione d'Impatto sulla Protezione dei Dati (DPIA) ai sensi dell'art. 35 GDPR. Per i sistemi classificati ad alto rischio ai sensi dell'AI Act, è altresi' obbligatoria la Valutazione d'Impatto sui Diritti Fondamentali (FRIA).

5. I log delle sessioni di utilizzo degli strumenti IA approvati, ove tecnicamente disponibili, sono conservati per un periodo minimo di 12 mesi, salva diversa previsione derivante dagli obblighi di conservazione dei procedimenti correlati, in conformità alle Linee guida AgID sulla conservazione documentale.

6. È istituito il Registro dei sistemi di Intelligenza Artificiale adottati da AIPo, tenuto a cura del Referente AI in raccordo con il RTD e con il DPO. Per ciascun sistema il Registro riporta, in particolare: denominazione e fornitore, finalità e processi supportati, classificazione del livello di rischio ai sensi degli artt. 6 e seguenti e dell'Allegato III del Regolamento (UE) 2024/1689 (AI Act), esito della DPIA e, ove dovuta, della FRIA, unità organizzativa titolare, data di adozione e di eventuale dismissione. Il Registro è aggiornato con cadenza almeno semestrale e costituisce la base informativa per gli adempimenti di cui al presente Regolamento.

7. Agli strumenti di IA si applicano le misure di sicurezza previste dal quadro normativo in materia di cybersicurezza, ed in particolare dalla Legge 28 giugno 2024, n. 90 e dal Decreto legislativo 4 settembre 2024, n. 138 (recepimento NIS2), nonché dalle indicazioni dell'Agenzia per la Cybersicurezza Nazionale (ACN), con particolare riguardo a: segmentazione delle reti, gestione degli accessi privilegiati, logging e monitoraggio, gestione delle vulnerabilità e degli incidenti. Gli incidenti significativi sono notificati al CSIRT Italia per il tramite del Referente per la cybersicurezza entro i termini previsti dalla normativa vigente (24/72 ore, secondo le rispettive fasi).

8. Il Referente AI, in raccordo con il RTD, il DPO e il Referente per la cybersicurezza, predispone un report annuale al Comitato di Indirizzo che illustra: i sistemi di IA in esercizio e quelli dismessi, gli incidenti e le anomalie rilevate, le attività di formazione erogate, le DPIA e le FRIA condotte, le azioni correttive e di miglioramento programmate.

9. Le violazioni del Regolamento possono comportare l'accertamento della responsabilità disciplinare secondo quanto previsto dal Codice di comportamento dell'Agenzia e dalla normativa vigente, fatta salva ogni ulteriore responsabilità civile, penale o amministrativa.

10. In caso di accertamento di violazioni, il Referente AI propone al RTD e al Direttore le misure idonee per la tutela della sicurezza o della protezione dei dati, ivi compresa l'eventuale segnalazione all'Autorità garante per la protezione dei dati personali, secondo le modalità previste dal Manuale di gestione degli incidenti informatici.

## ART. 8 — ENTRATA IN VIGORE E AGGIORNAMENTO

1. Il presente Regolamento entra in vigore con la pubblicazione presso il sito web istituzionale.

2. Il Regolamento è soggetto, a revisione annuale ed ogni qualvolta si verifichino modifiche normative rilevanti o evoluzioni tecnologiche significative che ne richiedano l'aggiornamento.

3. Le proposte di aggiornamento sono predisposte dal Referente AI, che supporta il RTD nella redazione delle modifiche tecniche. Le proposte sono sottoposte al Comitato di Indirizzo per l'approvazione.

4. Il Referente AI cura la comunicazione degli aggiornamenti del Regolamento a tutto il personale interessato, attraverso i canali istituzionali dell'Agenzia.

5. In sede di prima applicazione del presente Regolamento, è definita la seguente tempistica attuativa di massima:

- entro 60 giorni dall'entrata in vigore: pubblicazione della whitelist/blacklist iniziale
- entro 90 giorni: istituzione operativa del Registro dei sistemi di IA e censimento dei sistemi già in uso;
- entro 120 giorni: definizione del piano di formazione annuale differenziato per ruolo, con avvio dei percorsi obbligatori;
- entro 180 giorni: aggiornamento delle clausole contrattuali tipo per i fornitori di soluzioni IA e per le società in house, in coerenza con le clausole minime di cui all'art. 3, comma 5;
- entro 12 mesi: predisposizione del primo report annuale al Comitato di Indirizzo, ai sensi dell'art. 7.3, comma 8.

## ALLEGATO 1 — Esempi pratici di utilizzo: Ammesso / Non ammesso

La tabella seguente riporta un insieme di casistiche a titolo esemplificativo e non esaustivo circa l'ammissibilità o non ammissibilità dell'utilizzo degli strumenti IA nello svolgimento dell'attività lavorativa presso AIPo con gli specifici strumenti AI forniti dall'Agenzia.

| Esempio di utilizzo | Ammesso | Non ammesso | Note |
|---|---|---|---|
| Generare una bozza di e-mail istituzionale, poi rivista dal dipendente | ✓ | | Solo se verificata prima dell'invio |
| Usare l'IA per semplificare un testo tecnico destinato alla comunicazione pubblica | ✓ | | Richiede sempre verifica |
| Sintetizzare contenuti da fonti pubbliche ufficiali | ✓ | | La fonte deve essere verificabile |
| Redigere un piano di lavoro con supporto dell'IA (struttura, titoli, scaletta) | ✓ | | Va sempre validato dal responsabile |
| Generare automaticamente una risposta a un'istanza di parte e inviarla senza controllo | | ✗ | L'intervento umano è obbligatorio |
| Inserire in un prompt dati personali, riservati o credenziali di accesso | | ✗ | Viola GDPR e policy interne |
| Usare l'IA per decidere l'ammissibilità di un contributo o formulare una valutazione tecnica su opere idrauliche | | ✗ | I processi istruttori non possono essere automatizzati |
| Elaborare autonomamente dati di monitoraggio idrografico per reportistica ufficiale | | ✗ | I dati ambientali richiedono validazione umana obbligatoria |
| Creare contenuti in nome di altri uffici | | ✗ | Rischio di simulazione o manipolazione |
| Usare l'IA su account privato o dispositivo personale per compiti d'ufficio | | ✗ | Documenti interni e dati riservati non vanno condivisi con sistemi IA non approvati |
| Utilizzare l'IA per tradurre un documento pubblico o riformularlo in lingua semplificata | ✓ | | Utile, purché verificato |
| Redigere una presentazione con suggerimenti grafici e testuali generati dall'IA | ✓ | | Ammesso come supporto |
| Utilizzare l'IA per scrivere in autonomia verbali o atti ufficiali senza supervisione | | ✗ | Vietato: sostituisce attività a responsabilità personale |
| Impiegare l'IA durante l'orario di lavoro per fini personali | | ✗ | Utilizzo extraprofessionale non ammesso |
| Chiedere all'IA di proporre titoli alternativi a una relazione o documento informativo | ✓ | | Supporto utile per chiarezza comunicativa |
| Generare uno script o macro Excel per automatizzare un'attività ripetitiva | ✓ | | Ammesso se verificato dal Referente AI |
| Usare l'IA per generare contenuti per siti web istituzionali | ✓ | | Solo se i contenuti vengono revisionati da chi gestisce il sito |
| Caricare un documento interno o dati di monitoraggio del Po per farne riassumere il contenuto | | ✗ | Documenti interni e dati riservati non vanno condivisi con sistemi IA non approvati |

| Esempio di utilizzo | Ammesso | Non ammesso | Note |
|---|---|---|---|
| Far sintetizzare all'IA normative ambientali complesse per comprenderne l'impatto interno | ✓ | | Ammesso come supporto alla formazione, non per redazione ufficiale |
| Sottoporre all'IA una traccia per definire una policy interna o una linea guida tecnica | ✓ | | Utile per brainstorming, richiede sempre validazione |
| Utilizzare modelli predittivi di IA come supporto interno all'analisi di scenari di piena o eventi idrologici | ✓ | | Ammesso come supporto; la decisione finale resta sempre in capo al personale competente |
| Usare IA per pre-screening automatico di immagini da drone o da fonti satellitari relative a opere idrauliche | ✓ | | Ammesso per pre-screening; la validazione tecnica finale è sempre a cura del personale competente |
| Diffondere su canali istituzionali deepfake o contenuti sintetici (immagini, audio, video) non etichettati | | ✗ | Vietato ex art. 50 AI Act e L. 132/2025; i contenuti sintetici vanno sempre etichettati |
| Usare un assistente IA integrato (Copilot, Gemini, o analoghi) non presente in whitelist per attività d'ufficio | | ✗ | Strumento non autorizzato: occorre prima richiederne l'inserimento in whitelist al Referente AI |

*Per ulteriori chiarimenti sull'ammissibilità di specifici utilizzi non contemplati nella tabella, rivolgersi al Referente AI.*