

“Linee Guida per lo sviluppo di sistemi di Intelligenza Artificiale nella pubblica amministrazione”

“Linee Guida per il procurement di IA nella Pubblica Amministrazione”

adottate con la [Determinazione n.43/2026](#), in consultazione pubblica

fino all'11 aprile 2026

- 1) Il CSIG (Centro studi di informatica giuridica di Ivrea e Torino), segnala che tra i riferimenti normativi non si rinviene alcun richiamo del **New Legislative Framework (NLF)**, che influisce sui livelli di rischio, quadro legislativo che mira a migliorare il mercato interno dei prodotti e a rafforzare le condizioni per l'immissione sul mercato dell'UE di un'ampia gamma di prodotti. Si tratta di un insieme di misure volte a migliorare la sorveglianza del mercato e a incrementare la qualità delle valutazioni di conformità. Chiarisce inoltre l'utilizzo della marcatura CE e crea una serie di strumenti da impiegare nella legislazione sui prodotti. (cfr. https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en)
- 2) Il CSIG (Centro studi di informatica giuridica di Ivrea e Torino), segnala che tra i riferimenti normativi non si rinviene alcun richiamo all'art 4 dello Statuto dei lavoratori, che assume particolare rilevanza perché se l'analisi predittiva (sez. 3.2) viene applicata ai flussi di lavoro senza un accordo sindacale o autorizzazione dell'Ispettorato del Lavoro, si può configurare una violazione diretta del divieto di controllo a distanza dei lavoratori.
- 3) Il CSIG (Centro studi di informatica giuridica di Ivrea e Torino), segnala la mancanza di protocolli per la minimizzazione del dato nelle fasi di testing e validazione. Si suggerisce di imporre la separazione fisica e logica tra dati di training e dati operativi, privilegiando dati sintetici o anonimizzati per il fine-tuning.
- 4) Il CSIG (Centro studi di informatica giuridica di Ivrea e Torino) suggerisce di attenzionare la valutazione dei Principi di Sviluppo rispetto alla Sorveglianza Algoritmica. I 20 principi individuati nel capitolo 2.2 delle Linee Guida definiscono il perimetro etico-tecnico dello sviluppo, ma presentano ambiguità che potrebbero abilitare forme di sorveglianza occulta. Il Principio 2 (Rispetto dei valori fondamentali dell'UE), pur richiamando la CDFUE e l'AI Act (Reg. UE 1689/2024), rimane eccessivamente generico: la tutela dei diritti fondamentali nel contesto lavorativo italiano richiede riferimenti espliciti alle procedure di co-determinazione sindacale. Analogamente, il Principio 13 (Sorveglianza umana) rischia di essere ridotto a una verifica tecnica dell'output, ignorando la necessità di supervisionare la legittimità stessa del controllo esercitato dall'algoritmo sulla condotta del lavoratore. Un elemento di rischio inedito è rappresentato dalle Architetture Agentiche (sez. 2.1) e dall'Orchestratore (sez. 3.2.4). Se non correttamente vincolata, la logica di orchestrazione

può diventare il luogo dove vengono codificate regole di monitoraggio della performance in tempo reale, agendo come un supervisore automatizzato invisibile.

- 5) Il CSIG (Centro studi di informatica giuridica di Ivrea e Torino), segnala l'assenza di standard per le "Istruzioni per l'uso" richieste dall'Art. 13 dell'AI Act. Si suggerisce di esigere dai fornitori documentazione tecnica in formato "human-readable" che specifichi capacità, limiti e metriche di accuratezza del sistema.
- 6) Il CSIG (Centro studi di informatica giuridica di Ivrea e Torino) segnala la mancanza di distinzione tra protocolli HITL (Human-in-the-loop) e HOTL (Human-on-the-loop). Si suggerisce di definire procedure operative di override che consentano all'operatore di ignorare o invertire l'output algoritmico in tempo reale (Art. 14 AI Act).
- 7) Il CSIG (Centro studi di informatica giuridica di Ivrea e Torino) propone l'adozione obbligatoria del seguente protocollo in 5 punti per la conduzione congiunta di DPIA (GDPR) e FRIA (Fundamental Rights Impact Assessment - AI Act):
 1. Mappatura del Metodo Democratico: Valutare se il sistema può alterare processi decisionali pubblici o influenzare il comportamento degli utenti (conforme alla L. 132/2025).
 2. Audit dei Bias e Discriminazione: Analisi obbligatoria dei dataset per identificare pregiudizi algoritmici che violino la parità di trattamento.
 3. Verifica della Sovranità del Dato: Accertare la piena titolarità pubblica dei dataset e l'assenza di clausole di uso secondario non autorizzato da parte dei fornitori.
 4. Protocollo di Supervisione Umana: Definizione dei punti di controllo in cui l'intervento umano è necessario per convalidare decisioni ad alto impatto.
 5. Registro di Trasparenza: Conservazione dei log e delle versioni del modello per garantire la tracciabilità e la spiegabilità richieste dalle autorità di controllo.
- 8) Il CSIG (Centro studi di informatica giuridica di Ivrea e Torino) suggerisce l'adozione delle seguenti buone pratiche per la PA:
 1. Sanificazione continua dei Dataset: Implementazione di pipeline di validazione per prevenire l'iniezione di dati malevoli.
 2. Stress Testing di Accuratezza: Verifiche periodiche per misurare il degrado delle prestazioni in condizioni avverse.
 3. Segregazione degli Agenti: Nelle architetture orchestrate, ogni agente software deve operare secondo il principio del minor privilegio.
- 9) Il CSIG (Centro studi di informatica giuridica di Ivrea e Torino) suggerisce di prevedere le seguenti **Action Items ad Alto Impatto**:

1. **Emanazione di una Matrice di Responsabilità (RACI):** Definire uno schema standardizzato che ripartisca i compiti tra "Fornitore" (sviluppo/manutenzione) e "Utilizzatore" (gestione operativa), allineandolo ai ruoli previsti dall'AI Act per eliminare incertezze legali.
2. **Template Standardizzato del Technical File:** Produrre un modello di documentazione tecnica conforme agli allegati dell'AI Act, per facilitare le PA negli oneri di trasparenza e nelle attività di audit.
3. **Mandato di Efficienza Energetica e Fallback:** Inserire nei capitolati d'appalto KPI vincolanti sulla sostenibilità (Energy Layer) e l'obbligo tecnico di procedure di *fallback* su CPU, per garantire la resilienza nazionale di fronte a crisi di mercato o tecnologiche.

Bozza di linee guida per il procurement di IA nella Pubblica Amministrazione

- 1) Il CSIG (Centro studi di informatica giuridica di Ivrea e Torino, al fine di garantire il rispetto del divieto di sorveglianza dei lavoratori previsto dall'art. 4 dello Statuto dei lavoratori, suggerisce di inserire le seguenti clausole tipo per il Procurement (Riferimento Tabella 1):
 - "Il Fornitore DEVE garantire e certificare l'assenza di funzionalità di monitoraggio della performance lavorativa individuale o di analisi comportamentale nel codice e nelle logiche dell'Orchestratore."
 - "La PA si riserva il diritto di audit sui criteri di feature extraction dei modelli per verificare la conformità all'art. 8 L. 300/1970."

- 2) Il CSIG (Centro studi di informatica giuridica di Ivrea e Torino, con riferimento ai casi nei quali attraverso sistemi di IA vengano trattati dati personali, suggerisce di richiamare l'obbligo di designare il fornitore del sistema quale responsabile del trattamento di dati personali previsto dall'art. 28 del GDPR.

Inoltre, suggerisce di prevedere i seguenti requisiti Minimi per i Capitolati:

- Restituzione integrale: Obbligo di consegna di tutti i dati generati (output e metadati) in formati aperti e interoperabili al termine del contratto.
 - Portabilità tecnica: Garanzia di migrazione dei dataset verso altre infrastrutture senza oneri ingiustificati.
 - Divieto di riutilizzo non autorizzato: Clausole che impediscano al fornitore di utilizzare dati della PA per addestrare modelli esterni al servizio affidato.
- 3) Il CSIG (Centro studi di informatica giuridica di Ivrea e Torino, con riferimento al punto 3.4 Ruolo del dato nel procurement, suggerisce di integrare il principio di protezione dei dati personali prevedendo:
 - Lo sviluppo DEVE includere la Privacy by Design specifica per il contesto lavorativo. È fatto assoluto divieto di implementare funzionalità di monitoraggio costante e personalizzato. I dati identificativi dei lavoratori DEVONO essere pseudonimizzati nei log di sistema, rendendoli accessibili solo per motivate esigenze di sicurezza informatica.

Inoltre, segnala che la specificità normativa italiana (Artt. 4 e 8 L. 300/1970) richiederebbe i seguenti interventi correttivi:

- Definizione restrittiva di "Dati in Esercizio" (sez. 3.4.2) per escludere dati individuali
- Obbligo di coinvolgimento sindacale nella validazione (sez. 4.4)
- Divieto contrattuale di analisi predittiva della performance individuale
- Trasparenza sulla logica algoritmica dell'Orchestratore

4) Il CSIG (Centro studi di informatica giuridica di Ivrea e Torino, con riferimento agli obblighi di conformità alla NIS2 e ai provvedimenti di ACN suggerisce di prevedere che l'amministrazione, anche quando fa ricorso a servizi resi da terzi, deve assicurare una mappatura diretta tra le tassonomie di attacco e le "Buone pratiche" del paragrafo 5.7. A tal fine si indicano le seguenti azioni:

- Modellazione delle minacce (5.6.1): Identificazione dei punti di fallimento specifici negli input; validazione rigorosa dei vettori di attacco.
- Documentazione e Qualità dei Dati (5.6.5): Tracciabilità end-to-end della supply chain dei dati; audit sulla provenienza e integrità dei dataset di training.
- Analisi del Codice (5.6.2): Esecuzione di analisi statica e dinamica (SAST/DAST) focalizzata sulla prevenzione di data leakage via API.
- Security by Design (5.6.4): Implementazione di meccanismi di controllo degli accessi e segregazione dei ruoli lungo l'intero Stack.
- Approccio basato sul rischio (Principio 3 e Par. 5.2): deve tradursi in clausole contrattuali precise (Par. 6.4) prevedendo l'obbligo di esigere, in fase di gara, evidenze documentali su DPIA (valutazione d'impatto sulla protezione dei dati) e FRIA (valutazione d'impatto sui diritti fondamentali) per i sistemi ad alto rischio, evitando la coesistenza forzata tra dati pubblici e modelli proprietari opachi.

Infine, si segnala una lacuna riguardo agli obblighi di Notifica: la bozza non specifica la finestra di notifica di 72 ore (o i termini più stringenti per le pre-notifiche) prevista dal D.Lgs. 138/2024. Al riguardo si ritiene che le PA dovrebbero integrare autonomamente questo requisito nei protocolli di gestione incidenti per evitare sanzioni e garantire il coordinamento nazionale.