



ISTITUTO COMPRENSIVO "DE AMICIS – DON MILANI" - RANDAZZO -

RELAZIONE TECNICA DELL'AMMINISTRATORE DEL SISTEMA I.A.

Oggetto: Attestazione delle misure tecniche e organizzative adottate per l'utilizzo dei sistemi di Intelligenza Artificiale (Punto 7 del piano di campionamento/verifica).

Il sottoscritto, in qualità di Amministratore del Sistema IA, redige la presente relazione tecnica per attestare la conformità e le misure di sicurezza attivate in merito all'uso della piattaforma di Intelligenza Artificiale integrata nell'ecosistema aziendale/istituzionale.

1. Verifica del fornitore su catalogo ACN

In ottemperanza alle disposizioni vigenti in materia di infrastrutture cloud per la Pubblica Amministrazione e le aziende strategiche, si attesta che il fornitore del servizio cloud e delle funzionalità IA collegate è **Google**.

- **Stato di verifica:** Google Cloud / Google Workspace è regolarmente qualificato e inserito nel **Catalogo dei servizi Cloud della Agenzia per la Cybersicurezza Nazionale (ACN)**, garantendo i livelli di sicurezza, resilienza e conformità richiesti per il trattamento dei dati.

2. Addendum contrattuale (RdT ai sensi dell'Art. 28 GDPR)

Si conferma che i rapporti giuridici e di trattamento dati con il fornitore sono regolati in piena conformità al Regolamento UE 2016/679 (GDPR).

- **Stato di verifica:** È stato formalmente accettato e attivato all'interno della console di amministrazione Google il relativo **Addendum sul trattamento dei dati (Data Processing Addendum - DPA)**, che agisce come atto di nomina a Responsabile del Trattamento (RdT) ai sensi dell'Art. 28 GDPR. Tale accordo vincola il fornitore a trattare i dati personali esclusivamente per le finalità istituzionali/aziendali configurate, escludendo utilizzi terzi.

3. Conservazione dei prompt e della cronologia delle conversazioni

Al fine di garantire il principio di minimizzazione dei dati e ridurre il rischio di data leakage, si è provveduto a intervenire sulle impostazioni di memorizzazione delle sessioni.

- **Misure tecniche adottate:** All'interno della console di gestione dei servizi IA di Google, sono state **disattivate le funzionalità che consentono la conservazione centralizzata o persistente dei prompt inseriti dagli utenti e della cronologia delle conversazioni**. I dati di sessione

vengono gestiti in modalità volatile per il solo tempo strettamente necessario all'elaborazione della richiesta.

4. Esclusione del training dell'IA sulle chat degli utenti

Per tutelare la proprietà intellettuale, il segreto professionale e la riservatezza dei dati immessi nel sistema, è stata blindata la componente di apprendimento dell'algoritmo.

- **Misure tecniche adottate:** È stata applicata la policy di **disattivazione del training dei modelli di IA sulla base delle chat e dei dati degli utenti**. Google (nelle sue licenze Enterprise/Education e Google Cloud Vertex AI) garantisce contrattualmente che i dati aziendali, i prompt e le risposte generate non vengono utilizzati per addestrare, migliorare o perfezionare i modelli linguistici globali (LLM) del fornitore o di terze parti.

Conclusioni

Le misure sopra descritte soddisfano pienamente i requisiti minimi di sicurezza e compliance richiesti dal punto 7 del documento di riferimento, garantendo un uso presidiato, sicuro e conforme alla normativa privacy dell'Intelligenza Artificiale.

Randazzo 01/06/2026

Prof. Pagano Edoardo

