DPIA Google Workspace for Education - Appendice IA

IPSSAR “Pellegrino Artusi” di Riolo Terme

Integrazione specifica per l’adozione
degli strumenti di intelligenza artificiale generativa

Stato documento:	Definitivo
Versione:	1.0
Data ultimo aggiornamento	3 febbraio 2026

Indice

Indice 1
Art.1 - Panoramica del trattamento 2
Art.2 - Responsabilità connesse al trattamento 2
Art.3 - Standard applicabili al trattamento 4
Art.4 - Dati, processi e risorse di supporto 5
Art.5 - Proporzionalità e necessità 5
Art.6 - Misure a tutela dei diritti degli interessati 6
Art.7 - Misure esistenti o pianificate 6
Art.8 - Analisi dei rischi 7
Art.9 - Panoramica dei rischi 9

Art.1 - Panoramica del trattamento

La presente integrazione alla Valutazione di Impatto sulla Protezione dei Dati (DPIA) della piattaforma Google Workspace for Education riguarda l'estensione del trattamento dei dati personali mediante l'introduzione di strumenti di Intelligenza Artificiale (IA) generativa.

Nello specifico, il trattamento in esame consiste nell'attivazione e nell'uso didattico-organizzativo dei servizi Google Gemini e NotebookLM, nonché di ulteriori applicazioni di terze parti (il cui elenco verrà aggiornato dopo valutazione da parte della commissione IA e del dirigente) integrate nelle applicazioni didattiche e per specifici progetti.

Il trattamento si evolve dalla semplice archiviazione e condivisione di documenti verso una rielaborazione semantica e generativa dei contenuti. I sistemi di IA analizzano i dati inseriti dall'utente (prompt) e i documenti caricati come fonti per generare nuovi testi, immagini, analisi o sintesi.

L'istituto introduce tali strumenti per perseguire le seguenti finalità di pubblico interesse:

- Supporto alla didattica: Personalizzazione dell'apprendimento, supporto allo studio attraverso la semplificazione dei testi e la creazione di materiali inclusivi.
- Sviluppo delle competenze digitali: Educazione all'uso critico e responsabile dell'IA, in linea con le *Linee Guida del MIM* e l'*AI Act* europeo.
- Efficienza organizzativa: Automazione di compiti ripetitivi per il personale docente e ATA.

Il trattamento coinvolge dati identificativi e contenuti prodotti da studenti e personale scolastico. Rispetto alla DPIA originaria, il rischio si estende ai contenuti dei prompt e eventuali allegati ad essi, che potrebbero involontariamente contenere dati sensibili o dati personali non necessari, rendendo necessaria una nuova valutazione delle misure di sicurezza e delle istruzioni fornite agli utenti.

Art.2 - Responsabilità connesse al trattamento

La gestione dei dati personali attraverso sistemi di IA richiede una chiara definizione dei ruoli per garantire l'accountability e la protezione dei diritti degli interessati (studenti e personale), analogamente a quanto redatto per la Google Workspace for Education.

Il Titolare del trattamento è l'Istituzione Scolastica, rappresentata dalla figura del Dirigente Scolastica. Spetta al Titolare la responsabilità ultima di definire le finalità e i mezzi del trattamento, assicurando che l'adozione di strumenti quali Google Gemini e NotebookLM sia coerente con il PTOF e con i principi di privacy by design e by default. Il Titolare garantisce inoltre che siano stati sottoscritti gli opportuni atti di nomina con i fornitori e che la comunità scolastica sia adeguatamente informata.

I soggetti esterni che forniscono le piattaforme di IA (es. Google Ireland Ltd. per Workspace, Gemini e NotebookLM) agiscono in qualità di Responsabili del trattamento (ex Art. 28 GDPR). Essi hanno la responsabilità tecnica di trattare i dati secondo le istruzioni impartite dalla scuola, garantendo elevati standard di sicurezza e assicurando, nel caso dei servizi Education Core, che i dati inseriti non vengano utilizzati per l'addestramento dei propri modelli linguistici generali.

Il DPO dell'istituto svolge un ruolo di consulenza e sorveglianza. Le sue responsabilità specifiche nel contesto dell'IA includono:

- Fornire il parere sulla presente DPIA.
- Supportare il Titolare nel monitorare la conformità degli algoritmi e dei fornitori nel tempo e nella gestione di eventuali data breach derivanti dall'uso improprio di strumenti di IA generativa.

Il personale scolastico è designato come "Autorizzato al trattamento". I docenti hanno la responsabilità di:

- Supervisionare l'uso dell'IA da parte degli studenti (human-in-the-loop), assicurando che non sostituisca mai in toto la produzione di contenuti didattici e valutazione umana.
- Istruire gli alunni al rispetto della privacy, vietando l'inserimento di dati personali non necessari e dati sensibili nei prompt (es. informazioni sulla salute o sulla vita privata).
- Utilizzare esclusivamente le applicazioni e gli account istituzionali approvati dall'istituto.

Sebbene non siano responsabili del trattamento in senso giuridico, gli utenti sono chiamati a una responsabilità d'uso. Gli studenti devono attenersi al Regolamento di Istituto, integrato con il regolamento di utilizzo dell'IA, utilizzando le app esclusivamente per scopi didattici e nel rispetto della dignità altrui.

Si rimanda alla DPIA della Google Workspace for Education (già agli atti della presente Istituzione) per ulteriori dettagli e ad eventuali aggiornamenti in capo a Google stesso, presenti, nel dettaglio, ai seguenti link:

- **Termini di servizio di Google Workspace for Education (Generali):** Questo link contiene l'accordo principale tra l'istituto e Google, definendo obblighi e limitazioni di responsabilità. https://workspace.google.com/intl/it/terms/education_terms/
- **Informativa sulla Privacy di Google Workspace for Education:** Specifica quali dati vengono raccolti e come vengono utilizzati, sottolineando che per i servizi principali ("Core Services") i dati non vengono usati a fini pubblicitari. https://workspace.google.com/terms/education_privacy.html
- **Cloud Data Processing Addendum (CDPA):** È il documento fondamentale per la conformità al GDPR (Art. 28). Definisce il ruolo di Google come "Responsabile del trattamento" (Processor) e dell'istituto come "Titolare" (Controller). https://cloud.google.com/terms/data-processing-addendum
- **Addendum sui dati dei servizi per l'istruzione (Service Data Addendum):** Link specifico per le scuole che desiderano maggiore controllo sui dati di servizio generati dall'uso della piattaforma. https://workspace.google.com/terms/service-data-addendum/

Art.3 - Standard applicabili al trattamento

Il trattamento dei dati mediante le funzionalità di IA di Google Workspace e altre app didattiche avviene nel rispetto di un framework normativo e tecnico stratificato. Per quanto non espressamente indicato in questa sede, si rimanda integralmente agli standard di sicurezza già analizzati e documentati nella DPIA originaria di Istituto relativa a Google Workspace for Education.

Le infrastrutture utilizzate continuano a fare riferimento ai principali standard internazionali già validati nella DPIA principale:

- ISO/IEC 27018:2019: Codice di condotta per la protezione delle informazioni di identificazione personale (PII) nel cloud pubblico per i responsabili del trattamento.
- ISO/IEC 27001: Standard per la gestione della sicurezza delle informazioni.
- Standard contrattuali Google (SCCs): Il trattamento è disciplinato dal *Data Processing Amendment (CDPA)* di Google, che include le Clausole Contrattuali Standard approvate dalla Commissione Europea per il trasferimento dei dati verso paesi terzi.

In aggiunta agli standard citati nella DPIA originaria, l'integrazione delle app di IA considera i seguenti riferimenti emergenti:

- Regolamento UE 2024/1689 (AI Act): Il trattamento è configurato per rispettare i requisiti di trasparenza (art. 50) e per evitare pratiche di IA vietate, classificando gli strumenti didattici in uso come sistemi a rischio contenuto o basso, purché soggetti a supervisione umana.
- Linee Guida del Gruppo di Lavoro Art. 29 / EDPB: In particolare per quanto riguarda il processo decisionale automatizzato e la profilazione (Art. 22 GDPR), assicurando che l'IA sia usata solo come supporto e mai come unico criterio di valutazione dello studente.
- NIST AI Risk Management Framework (AI RMF): Google adotta l'approccio basato sul rischio per garantire che i sistemi di IA siano affidabili, sicuri e privi di bias discriminatori.

Il trattamento si uniforma inoltre alle Linee guida etiche sull'uso dell'intelligenza artificiale e dei dati nell'insegnamento e nell'apprendimento per gli educatori della Commissione Europea, che definiscono i criteri di equità, umanità e tutela del benessere del minore e che vengono riportate nell'integrazione al Regolamento di Istituto in cui vengono descritte le norme di utilizzo dell'IA attraverso l'account scolastico.

Art.4 - Dati, processi e risorse di supporto

Il trattamento riguarda i dati identificativi di studenti e personale, come nomi ed email istituzionali, unitamente ai contenuti generati dagli utenti sotto forma di prompt, testi, immagini e sintesi analitiche. Il ciclo di vita del dato inizia con l'inserimento di istruzioni o documenti nelle interfacce di IA come Gemini e NotebookLM, prosegue con la rielaborazione generativa dei contenuti e si conclude con l'archiviazione sicura all'interno del tenant Google Workspace dell'istituto fino alla cancellazione per cessazione dell'account o richiesta dell'utente. Le risorse di supporto comprendono l'infrastruttura cloud di Google, protetta da hardware personalizzato e sistemi operativi ottimizzati per la sicurezza, oltre ai dispositivi scolastici o personali autorizzati che accedono alla rete tramite protocolli cifrati HTTPS e TLS.

Gli interessati ricevono informazioni sul trattamento attraverso l'informativa pubblicata sul sito istituzionale e le integrazioni al Regolamento di Istituto che descrivono le norme di utilizzo dell'IA. Il trattamento principale non richiede il consenso poiché basato sull'interesse pubblico, tuttavia l'istituto assicura la trasparenza necessaria affinché gli utenti possano esercitare i diritti di accesso e portabilità tramite strumenti come Google Takeout o rivolgendosi al Titolare. I diritti di rettifica, cancellazione, limitazione e opposizione, e tutti i diritti di cui al capo III GDPR, possono essere esercitati contattando formalmente il titolare del trattamento per il tramite del Dirigente Scolastico o del DPO dell'istituto. Gli obblighi dei responsabili esterni sono disciplinati rigorosamente dal Data Processing Amendment di Google, che include le Clausole Contrattuali Standard approvate dalla Commissione Europea per garantire una protezione equivalente in caso di trasferimento dei dati al di fuori dell'Unione Europea

Art.5 - Proporzionalità e necessità

Gli scopi del trattamento sono definiti in modo specifico e legittimo, mirando al supporto della didattica personalizzata, all'efficienza organizzativa e allo sviluppo di competenze digitali critiche in linea con l'AI Act europeo. La base legale risiede nell'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investita l'Istituzione Scolastica, coerentemente con il PTOF e le linee guida del MIM. Per garantire la minimizzazione, il trattamento è limitato ai dati necessari alla generazione degli output e il personale deve istruire gli alunni a non inserire dati sensibili nei prompt. L'esattezza dei dati è garantita dal monitoraggio contro bias discriminatori,

sebbene l'output richieda sempre la supervisione umana secondo il principio di human-in-the-loop. Il periodo di conservazione coincide con la durata della carriera scolastica o del rapporto lavorativo, fatti salvi i diritti di cancellazione.

Art.6 - Misure a tutela dei diritti degli interessati

Per quanto riguarda le misure a tutela dei diritti degli interessati, l'istituto garantisce la massima trasparenza fornendo informazioni dettagliate sul trattamento attraverso l'informativa pubblicata sul sito web istituzionale e le integrazioni specifiche al Regolamento di Istituto che disciplinano l'uso corretto dell'Intelligenza Artificiale tramite l'account scolastico. Poiché l'adozione di tali strumenti avviene per il perseguimento di finalità di pubblico interesse legate alla didattica e allo sviluppo delle competenze digitali, il trattamento non richiede solitamente il consenso preventivo, ma resta ferma la possibilità per gli studenti di ricevere chiarimenti o autorizzare progetti extra-curriculari specifici.

Gli interessati possono esercitare agevolmente i propri diritti di accesso e portabilità dei dati attraverso le funzionalità tecniche native della piattaforma, inviando una richiesta formale al Dirigente Scolastico, che agisce in qualità di Titolare del trattamento. Allo stesso modo, i diritti di rettifica, cancellazione, limitazione e opposizione vengono garantiti mediante la possibilità per l'utente di gestire la propria cronologia delle attività all'interno delle applicazioni o di richiedere l'intervento diretto dell'istituto o del Responsabile della protezione dei dati per le operazioni più complesse.

Tutti gli obblighi in capo ai fornitori esterni, che agiscono come Responsabili del trattamento, sono definiti con estrema chiarezza e disciplinati da appositi contratti, come il Data Processing Amendment di Google, che vincola il fornitore a trattare i dati esclusivamente secondo le istruzioni della scuola e per scopi didattici. Infine, la protezione dei dati è assicurata anche in caso di trasferimento al di fuori dell'Unione Europea grazie all'adozione delle Clausole Contrattuali Standard approvate dalla Commissione Europea, le quali garantiscono standard di sicurezza e tutele giuridiche equivalenti a quelli previsti dal regolamento europeo.

(Per l'esercizio dei diritti si rimanda al paragrafo precedente.)

Art.7 - Misure esistenti o pianificate

- **Formazione del personale e conformità al regolamento di istituto**

  Al fine di garantire che l'integrazione degli strumenti di Intelligenza Artificiale avvenga nel pieno rispetto dei diritti degli interessati, l'istituto pianifica e attua programmi di formazione specifica rivolti a tutto il personale docente. Tali interventi formativi sono focalizzati sull'uso corretto e responsabile dei sistemi di IA e sulle implicazioni privacy connesse all'uso dell'IA generativa, con particolare attenzione alla prevenzione del data leakage e al divieto di inserimento di dati sensibili o particolari all'interno dei prompt. Il personale è inoltre tenuto all'osservanza rigorosa del Regolamento di Istituto, che viene periodicamente aggiornato per includere le norme di comportamento etico e sicuro nell'interazione con le tecnologie emergenti. Questa misura mira a creare una cultura della responsabilità (accountability) diffusa, assicurando che ogni operatore sia consapevole dei rischi e agisca in conformità con le policy di sicurezza stabilite, riducendo così drasticamente la probabilità di violazioni derivanti da errori umani o usi impropri della piattaforma.

- **Crittografia**

  Nei data center di Google i dati at-rest sono cifrati per impostazione predefinita. I dati sono protetti con più livelli di sicurezza che includono tecnologie di crittografia all'avanguardia, come i protocolli HTTPS e Transport Layer Security. I data center di Google utilizzano un hardware personalizzato su cui sono in esecuzione un sistema operativo e un file system

protetti personalizzati. Ciascuno di questi sistemi è stato ottimizzato per la sicurezza e le prestazioni. Dal momento che Google controlla tutto l'hardware, è possibile reagire rapidamente a qualsiasi minaccia o all'eventuale individuazione di punti deboli. Inoltre tutti gli accessi alla piattaforma Google Workspace for Education sono protetti da credenziali di autenticazione che sono attribuite e gestite su base strettamente nominativa ed individuale.

- **Controllo degli accessi**

  Nella piattaforma Google tutti i prodotti sono protetti in modo continuo da un'adeguata infrastruttura di sicurezza, completamente ridondata e fault-tolerant, cosicché è possibile resistere efficacemente a tutti i tentativi illeciti di accedere ai dati. Il meccanismo di sicurezza integrata di Google rileva le minacce tramite sofisticati meccanismi e strumenti di Intrusion Detection ed interviene preventivamente per eliminare o contrastare le minacce ancora prima che queste possano causare danni o perdita di riservatezza delle informazioni.

Art.8 - Analisi dei rischi

L'analisi dei rischi contenuta nella presente integrazione è stata condotta adottando la metodologia e i criteri definiti dal software ufficiale messo a disposizione dal Garante per la Protezione dei Dati Personali. Tale approccio ha permesso di valutare in modo sistematico le vulnerabilità connesse all'introduzione degli strumenti di Intelligenza Artificiale, strutturando l'esame attorno a tre direttrici fondamentali per la sicurezza delle informazioni. Nello specifico, la valutazione analizza nel dettaglio gli scenari relativi al rischio di accesso illegittimo ai dati, inteso come violazione della riservatezza, alle modifiche indesiderate dei dati, che attengono alla sfera dell'integrità e dell'esattezza delle informazioni, e alla perdita dei dati, volta a garantire la continuità e la disponibilità del patrimonio informativo dell'istituto e degli interessati.

8.1 - Analisi dei rischi: accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare? Perdita di riservatezza: divulgazione non autorizzata di dati personali o contenuti didattici, Esposizione di dati sensibili: i "prompt" inseriti dagli utenti potrebbero contenere involontariamente opinioni personali o dati particolari. Compromissione della riservatezza: l'esposizione di "prompt" o documenti caricati potrebbe rivelare opinioni personali, dati sensibili o dinamiche private espresse in un ambiente ritenuto protetto. Profilazione algoritmica non autorizzata: l''accesso ai dati analizzati dall'IA permetterebbe a terzi di ricostruire un profilo dettagliato delle capacità cognitive, delle fragilità e degli stili di apprendimento dei minori, con il pericolo di future discriminazioni o catalogazioni improprie del loro percorso formativo; Google non profila i prompt inseriti. Sicurezza digitale e psicologica: la perdita di controllo sulle proprie informazioni (nomi, abitudini, contenuti creativi) può facilitare furti d'identità e generare un profondo senso di insicurezza. Inibizione della libertà di espressione a causa di eccessivo timore, portando utenti e docenti all'autocensura nell'uso delle tecnologie didattiche, limitando di fatto il diritto a una sperimentazione educativa libera e consapevole.

Quali sono le principali minacce che potrebbero concretizzare il rischio? Cyber-attacchi: tentativi illeciti di violare l'infrastruttura o intercettazione del traffico di rete, Fattore umano: utilizzo di credenziali deboli o mancata disattivazione di account non più autorizzati, Vulnerabilità software: sfruttamento di bug nei sistemi operativi o nelle applicazioni

Quali sono le fonti di rischio? Attori esterni: hacker o terze parti malintenzionate, Errori interni: personale o studenti che utilizzano password inadeguate o canali non protetti

Quali misure fra quelle individuate contribuiscono a mitigare il rischio? Crittografia, Controllo degli accessi, Formazione del personale e conformità al regolamento di istituto

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate? Limitata, gli impatti sono potenzialmente significativi per la privacy, ma limitati dalla natura dei dati trattati (prevalentemente didattici)

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate? Trascurabile, le misure tecniche di Google (cifratura, sicurezza fisica) rendono molto difficile un accesso massivo ai dati

8.2 - Analisi dei rischi: modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare? Danno reputazionale attraverso la generazione di contenuti inappropriati

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio? Accessi non autorizzati: manipolazione di file o cartelle da parte di chi ha ottenuto permessi impropri, Prompt Injection: inserimento di istruzioni malevole per forzare l'AI a produrre output errati o dannosi

Quali sono le fonti di rischio? Utenti autorizzati: modifiche accidentali o volontarie ai documenti condivisi

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio? Crittografia, Controllo degli accessi, Formazione del personale e conformità al regolamento di istituto.

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate? Trascurabile, le modifiche possono essere rilevate e corrette tramite la cronologia delle revisioni

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate? Trascurabile, grazie ai meccanismi di controllo degli accessi e ai log di sistema

8.3 - Analisi dei rischi: perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi? Esposizione di dati sensibili: i "prompt" inseriti dagli utenti potrebbero contenere involontariamente opinioni personali o dati particolari, Interruzione della didattica: impossibilità di accedere a materiali, compiti o strumenti AI, Perdita di lavoro: distruzione accidentale o illecita di contenuti generati da studenti o docenti

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio? Cancellazione accidentale: errore umano nell'eliminazione di file o interi account, Eventi catastrofici: incendi, inondazioni o guasti hardware critici nei data center

Quali sono le fonti di rischio? Fornitore del servizio: interruzioni tecniche o problemi infrastrutturali del cloud, Ambiente: calamità naturali che colpiscono i siti di conservazione fisica

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio? Crittografia, Controllo degli accessi, Formazione del personale e conformità al regolamento di istituto.

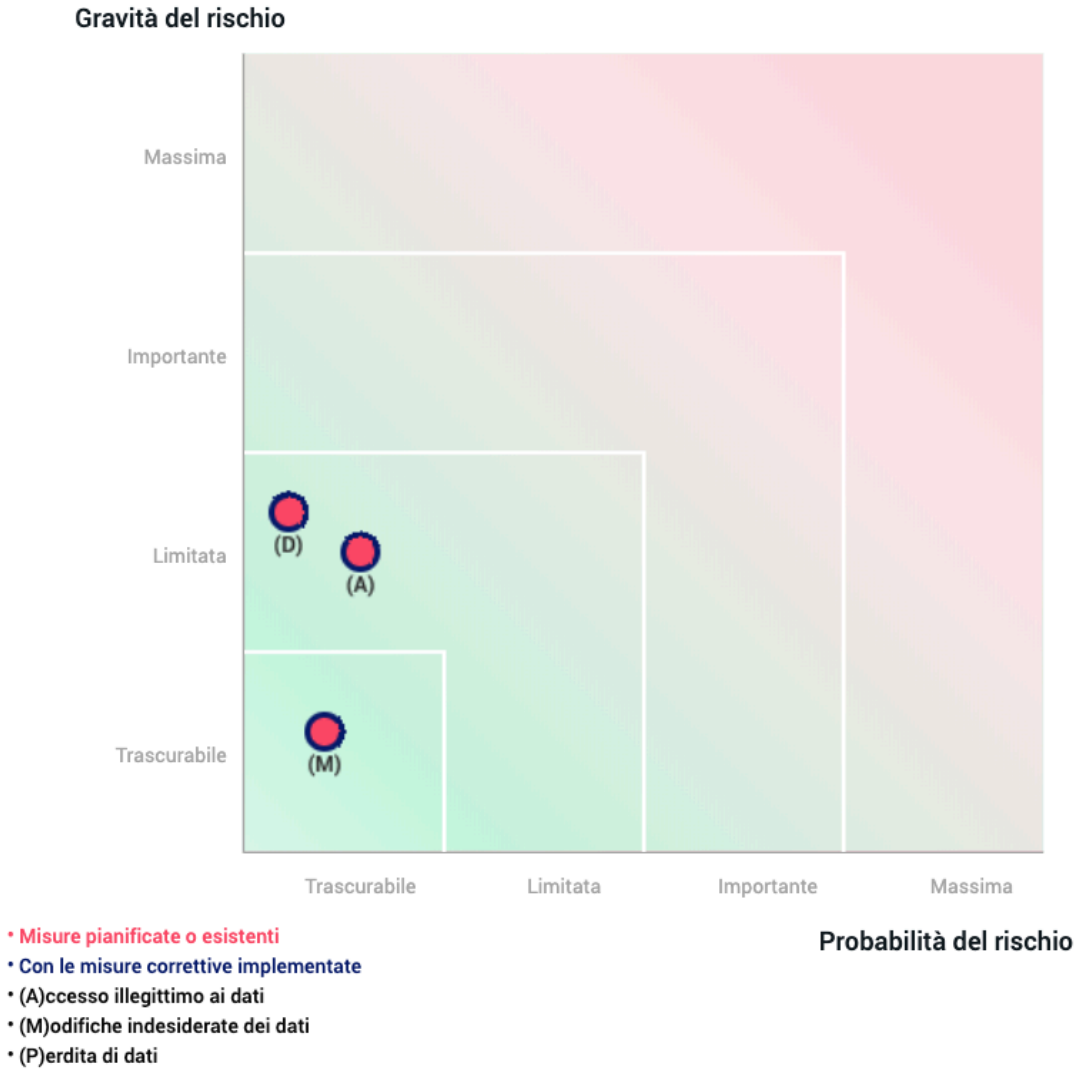
Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate? Limitata,la perdita definitiva avrebbe un impatto per il lavoro svolto ma non ne comprometterebbe il percorso e il recupero è quasi sempre possibile

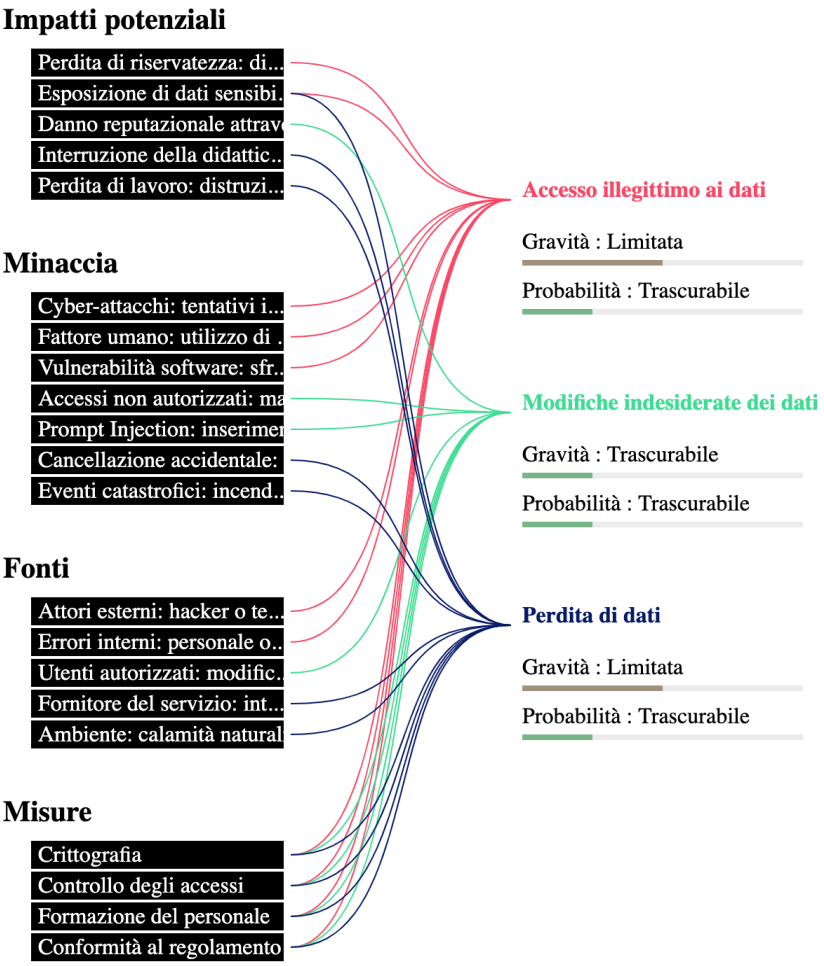
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate? Trascurabile, l'architettura cloud ridondata di Google è progettata per una disponibilità prossima al 100%

Art.9 - Panoramica dei rischi

A corredo dell'analisi metodologica, viene di seguito riportata la rappresentazione grafica della panoramica dei rischi, elaborata attraverso l'impiego del software ufficiale del Garante per la Protezione dei Dati Personali. Tale illustrazione sintetizza visivamente il posizionamento delle diverse tipologie di rischio analizzate — accesso illegittimo, modifiche indesiderate e perdita dei dati — mettendone in relazione la gravità del potenziale impatto con la probabilità che l'evento minaccioso si verifichi.

La mappatura così ottenuta evidenzia come l'azione combinata delle misure di sicurezza tecniche offerte dalla piattaforma e delle misure organizzative adottate dall'Istituto permetta di mantenere il rischio residuo entro livelli di accettabilità, garantendo una tutela efficace dei diritti e delle libertà degli interessati anche nell'utilizzo di sistemi di intelligenza artificiale.




Impatti potenziali
Perdita di riservatezza: di...
Esposizione di dati sensibi..
Danno reputazionale attrav
Interruzione della didattic..
Perdita di lavoro: distruzi...
Minaccia
Cyber-attacchi: tentativi i...
Fattore umano: utilizzo di .
Vulnerabilità software: sfr..
Accessi non autorizzati: ma
Prompt Injection: inserimer
Cancellazione accidentale:
Eventi catastrofici: incend..
Fonti
Attori esterni: hacker o te..
Errori interni: personale o..
Utenti autorizzati: modific..
Fornitore del servizio: int...
Ambiente: calamità natural
Misure
Crittografia
Controllo degli accessi
Formazione del personale
Conformità al regolamento
Accesso illegittimo ai dati
Gravità : Limitata
Probabilità : Trascurabile
Modifiche indesiderate dei dati
Gravità : Trascurabile
Probabilità : Trascurabile
Perdita di dati
Gravità : Limitata
Probabilità : Trascurabile