DOSSIER TECNICO-NORMATIVO

CHATBOT CLOUD, API CON RETENTION CONTROLLATA E IA LOCALE

Protezione dei dati, tracciamento delle chiamate e architetture sicure per scuole, PA e imprese

Edizione pubblica verificata

A cura di Francesco Silvaggio e del Team di Orizzonte Insegnanti

Aggiornato al 27 luglio 2026

PREMESSA

Obiettivo, tesi e metodo della ricerca

Un dossier sulle architetture e sul percorso dei dati, non una campagna contro l'IA.

✓ **TESI CENTRALE**

In questo dossier si adotta una regola organizzativa prudenziale: i chatbot consumer in cloud non vanno utilizzati con dati personali, riservati o segreti. Non è un divieto normativo generalizzato, ma una scelta di governance coerente con minimizzazione e privacy by default. Per l'uso organizzativo è preferibile un'applicazione controllata che chiami API con garanzie documentate di no-training e retention minima o nulla; per i dati più sensibili è preferibile l'inferenza locale o un ambiente privato, purché telemetria, egress e log di contenuto siano realmente disattivati.

Il problema non è che ogni servizio cloud utilizzi automaticamente ogni prompt per addestrare il modello. Il problema è che, quando un dipendente usa una chat pubblica, l'organizzazione perde il controllo tecnico e contrattuale sul trattamento: quali dati sono inviati, quali log sono generati, per quanto tempo rimangono, chi può esaminarli, quali funzioni stateful o connettori li copiano altrove e quali trasferimenti internazionali si producono.

Il dossier distingue quattro modelli: chatbot consumer; SaaS enterprise; API attraverso un gateway organizzativo; IA locale o on-premise. La distinzione è decisiva, perché "cloud", "business", "API", "no-training" e "zero data retention" non sono sinonimi.

La ricerca usa fonti primarie: GDPR ed EUR-Lex, Garante per la protezione dei dati personali, EDPS, EDPB, NIST, NCSC, OWASP e documentazione ufficiale dei fornitori. Le fonti sono state ricontrollate il 27 luglio 2026 e le variazioni rilevanti sono già integrate nel corpo del dossier; il registro finale rende tracciabili gli aggiornamenti. Sono escluse percentuali promozionali prive di una fonte primaria riproducibile.

Trasparenza sul metodo. Orizzonte Insegnanti sviluppa applicazioni che accedono a modelli di terzi tramite API e backend dedicati. Il dossier non considera questa scelta una certificazione di sicurezza: separa le garanzie documentate dal provider, le opzioni di retention effettivamente attive e i controlli applicativi da verificare. Una richiesta ZDR inviata, un account a pagamento o una chiave associata a Cloud Billing non equivalgono a ZDR attivo; tale stato va dichiarato solo dopo conferma del fornitore e verifica della configurazione. Alla data del 27 luglio 2026, non risulta ancora una conferma di attivazione delle richieste ZDR avviate da Orizzonte Insegnanti; il dossier non le presenta quindi come garanzie attive.

! **CORREZIONE NECESSARIA**

API non significa automaticamente "nessuna traccia": retention e condivisione dipendono da provider, modello, endpoint, funzione, contratto e configurazione. Abuse monitoring, application state, cache, file, conversazioni, thread, vector store, grounding e strumenti esterni possono seguire cicli distinti. Zero Data Retention non è una certificazione generale del provider: è una condizione contrattuale e tecnica circoscritta a organizzazione o progetto, modello, endpoint, funzione e configurazione. Anche "IA locale" non significa automaticamente sicurezza: logging, telemetria, backup, RAG, accessi ed egress devono essere configurati e verificati.

Fonti chiave: [R1] GDPR; [R2] EDPS; [R4] NIST AI 600-1; [R5] NCSC; [R8-R9] Garante privacy e scuola; [P3] OpenAI API Data Controls; [P7-P8, P12] Anthropic retention/ZDR; [P9-P11, P13] Microsoft, Google Cloud e AWS; [P14-P15] Gemini Developer API: Paid Services e ZDR.

Mappa del dossier

Sezione	Domanda a cui risponde
1. Modelli di utilizzo	Che differenza c'è tra chat pubblica, SaaS enterprise, API controllata e IA locale?
2. Minacce	Dove possono finire prompt, file, log, metadati, dati RAG e connettori?
3. Evidenze	Cosa dichiarano le policy ufficiali su training, retention, revisione e storage stateful?
4. Quadro GDPR	Quali obblighi ricadono su titolare, DPO, IT e responsabili del trattamento?
5. Architetture	Come progettare un gateway API e un ambiente locale realmente controllati?
6. Decisione	Quale soluzione usare in funzione della sensibilità del dato?

Sezione	Domanda a cui risponde
7-8. Attuazione	Quali requisiti inserire in capitolato, policy, collaudo e piano 30-60-90 giorni?

SINTESI

Executive summary

Sette conclusioni operative supportate dalle fonti.

1. La chat consumer è un canale esterno di trattamento. Prompt, file, immagini, audio, video, dati dei servizi collegati e metadati sono trattati secondo condizioni consumer. L'organizzazione non dispone di un perimetro tecnico centralizzato né di garanzie equivalenti a un DPA enterprise. [P1-P5]

2. Revisione umana e retention non sono ipotesi astratte. Google invita a non inserire informazioni confidenziali che non si vorrebbero mostrare a un revisore e indica periodi fino a tre anni per conversazioni già revisionate. OpenAI e Anthropic prevedono retention ed eccezioni di sicurezza o legali. [P1, P4-P5]

3. No-training non equivale a zero retention. Un provider può non addestrare i modelli sui dati del cliente e, nello stesso tempo, conservare contenuti per abuse monitoring, file, funzioni stateful, feedback, supporto, obblighi legali o regole specifiche del modello. [P3, P6-P10, P12-P13]

4. L'API è preferibile solo se è controllata. L'API permette di imporre identità, finalità, DLP, pseudonimizzazione, allowlist di endpoint, retention verificata e audit senza contenuto. Senza questi controlli una webapp può replicare i rischi della chat pubblica registrando prompt e risposte nei propri log. [R4, R6, P3, P7-P10]

5. L'IA locale offre la maggiore sovranità del dato. Se il runtime non ha egress, la telemetria è disattivata e prompt, embeddings e documenti RAG restano nell'infrastruttura dell'ente, il contenuto non viene trasmesso a un provider di modello. Rimangono rischi interni, di supply chain, accesso, patching e backup. [R4, R5, R7]

6. GDPR e AI Act impongono progettazione, prova e obblighi distinti ma concorrenti. Minimizzazione, privacy by design/default, sicurezza, contratto con il responsabile, DPIA, trasparenza e controllo dei trasferimenti devono essere documentati. La configurazione effettiva va verificata, non solo promessa. [R1-R3, R8-R11]

7. Per scuola e PA la cautela deve essere più alta. Dati di minori, salute, disabilità, BES/DSA, PEI/PDP, valutazioni, procedimenti e dati dei dipendenti possono essere particolarmente delicati. In questo dossier si raccomanda, come regola organizzativa prudenziale e non come divieto normativo generalizzato, di vietare la chat consumer con dati non pubblici; l'API richiede un percorso formalizzato e il locale è preferibile per le classi più sensibili.

✓

RACCOMANDAZIONE DI DEFAULT

Adottare, previa valutazione del caso d'uso, un modello "API-first, local-when-sensitive": API enterprise dietro gateway per i casi ordinari, con retention minima/ZDR e nessun log di contenuto; inferenza locale o privata per categorie particolari di dati, minori, dossier individuali, segreti industriali, contenzioso e documentazione la cui divulgazione causerebbe un danno significativo. È una raccomandazione tecnico-organizzativa da adattare a finalità, base giuridica, DPIA, contratto e configurazione effettiva.

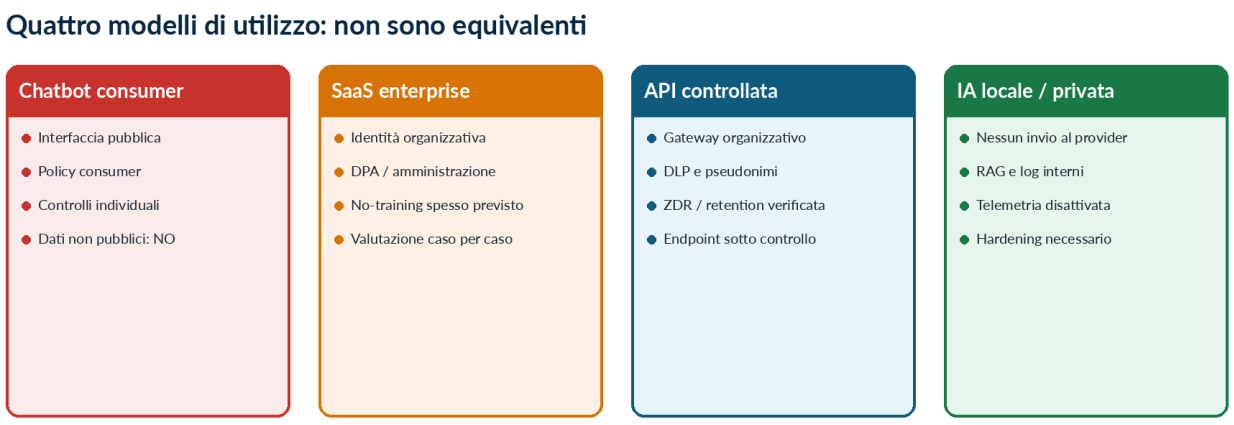

Figura 1 - I quattro modelli devono essere valutati separatamente.

SEZIONE 1

I quattro modelli di utilizzo

Per giudicare il rischio bisogna identificare chi tratta il dato, con quale contratto e con quali funzioni.

1.1 Chatbot consumer in cloud

È il servizio utilizzato direttamente da un individuo tramite sito o app pubblica. Account, impostazioni, cronologia e connettori sono governati dalla policy consumer. L'organizzazione può vietarne l'uso, ma spesso non può verificare centralmente quali prompt siano inviati né garantire che ogni dipendente abbia configurato correttamente opt-out, chat temporanee e cancellazioni.

- Il contenuto può comprendere prompt, allegati, immagini, audio, video, codice, URL e dati provenienti da servizi collegati.
- Possono essere raccolti log di utilizzo, dati del dispositivo, indirizzi IP, identificatori e informazioni di posizione o feedback.
- Training, revisione umana e retention dipendono dalla policy e dalle impostazioni del singolo servizio.
- La cancellazione dall'interfaccia non implica necessariamente eliminazione immediata da ogni sistema o da contenuti già dissociati.

✕	**REGOLA** Nel modello organizzativo proposto, la chat consumer è ammessa soltanto per informazioni pubbliche, contenuti sintetici o testi già anonimizzati in modo robusto. Non va usata per dati di terzi non pubblici.

1.2 SaaS enterprise

È una chat gestita in un tenant aziendale o scolastico, con amministrazione centralizzata, identità organizzative e condizioni commerciali. Può offrire, in funzione del piano e del contratto, no-training, DPA, audit, gestione degli utenti e controlli di retention. Rimane però un servizio cloud: il contenuto è processato dal fornitore e può essere conservato da funzioni stateful, sistemi di sicurezza, connettori o impostazioni dell'amministratore.

1.3 API attraverso un gateway organizzativo

L'utente non accede al fornitore. Usa una webapp dell'ente che applica controlli prima e dopo la chiamata: autenticazione, autorizzazione, filtro DLP, pseudonimizzazione, limite di finalità, selezione dell'endpoint, disattivazione dello storage, filtro dell'output e audit tecnico. L'invio al provider non scompare, ma diventa un trattamento controllato dall'amministrazione.

Questo è il modello raccomandato per la maggior parte dei casi organizzativi solo dopo una valutazione del trattamento e quando le garanzie di retention sono provate per lo specifico progetto, modello, endpoint e funzione. "OpenAI API", "Anthropic API", "Gemini Developer API" o un servizio Gemini su Google Cloud non sono configurazioni uniche né intercambiabili: conversazioni, file, thread, vector store, grounding e cache possono avere retention diversa.

1.4 IA locale, on-premise o privata

Il modello viene eseguito su server, workstation o infrastruttura privata controllata dall'organizzazione. Prompt, output, embeddings e documenti RAG possono restare nel perimetro locale. Il vantaggio è architetturale: non è necessario trasmettere il contenuto a un provider esterno per ottenere l'inferenza. Perché questa proprietà sia reale, occorre disattivare telemetria e crash reporting, impedire l'egress del processo, verificare il codice e i pesi, evitare log di prompt e risposta, proteggere il vector database, cifrare dischi e backup e applicare RBAC e patching.

Caratteristica	Consumer	SaaS enterprise	API controllata	Locale / on-prem
Controllo organizzativo	Basso	Medio-alto	Alto	Potenzialmente massimo
No-training	Dipende da opt-out	Spesso contrattuale	Contrattuale/configurabile	Intrinseco se nessun invio
Zero retention	In genere no	Dipende dal piano	Possibile ma da verificare	Possibile sotto controllo interno
DLP prima dell'invio	No	Limitato/variabile	Sì	Sì
Connettori e strumenti	Scelti dall'utente	Gestibili dall'admin	Allowlist applicativa	Gestiti internamente
Dati ad alta sensibilità	Vietati	Solo eccezioni valutate	Condizionata a DPIA/ZDR	Preferibile, con hardening

SEZIONE 2

Pericolosità e modello di minaccia

Il rischio non si esaurisce nell'addestramento del modello.

2.1 Il prompt è una comunicazione di dati a un sistema esterno

Quando nel prompt compaiono nome, diagnosi, valutazione, codice sorgente, contratto, credenziale o documento interno, il trattamento non riguarda soltanto la frase digitata. Include il contenuto, il contesto della conversazione, gli allegati, gli identificatori di account, i metadati tecnici e, in presenza di strumenti, i dati recuperati da altre fonti.

NIST definisce il rischio di data privacy della generative AI in termini di leakage, uso o divulgazione non autorizzata e de-anonimizzazione di dati personali o sensibili. OWASP include tra le informazioni esposte PII, dati finanziari e sanitari, credenziali, documenti legali e dati aziendali confidenziali. [R4, R6]

2.2 Otto vettori da considerare separatamente

Vettore	Perché è rilevante
Contenuto in ingresso	Prompt, file, immagini, audio, URL e parti di documenti possono contenere dati personali o segreti non necessari alla finalità.
Retention del provider	Il contenuto può restare in abuse monitoring, sistemi di sicurezza, cronologia, cache o storage applicativo per periodi diversi.
Training e miglioramento	Le versioni consumer possono usare conversazioni per migliorare i modelli, salvo impostazioni o eccezioni; i servizi commerciali possono escluderlo per contratto.
Revisione umana	Alcuni provider dichiarano revisione di una quota di dati, soprattutto per qualità, sicurezza o violazioni delle policy.
Log dell'applicazione cliente	Reverse proxy, APM, Sentry, tracing, database, queue e backup possono conservare prompt e risposte anche quando l'API dichiara ZDR.
Funzioni stateful	Conversazioni, thread, assistants, file, vector store, cache e cronologie possono avere una retention distinta dall'inferenza stateless.
Connettori e agenti	Web search, email, drive, browser, MCP e tool esterni aggiungono altri titolari/responsabili, policy e percorsi di esfiltrazione.
Prompt injection e RAG	Contenuti esterni possono impartire istruzioni al modello, spingerlo a rivelare dati del contesto o usare strumenti oltre la finalità. [R7]

2.3 Metadati: "non salvo il testo" non significa "non traccio la chiamata"

Anche eliminando prompt e risposta, un sistema può registrare utente, timestamp, IP, organizzazione, modello, token, latenza, classificazioni di sicurezza, endpoint, file ID, errori e identificatori di richiesta. Questi metadati possono essere necessari per sicurezza e fatturazione, ma devono essere distinti dal contenuto e sottoposti a una retention definita.

> **OBIETTIVO CORRETTO**
> Per "non tenere traccia dei dati e delle chiamate" è opportuno intendere: nessun prompt, output o allegato nei log; nessuna cronologia applicativa non necessaria; storage stateful disattivato; metadati tecnici ridotti al minimo e conservati per un periodo documentato. Un audit completamente assente può essere incompatibile con sicurezza e accountability.

2.4 Perché i filtri testuali non bastano

Una regola nel system prompt del tipo “non rivelare dati riservati” è utile ma non è una barriera di sicurezza. OWASP osserva che le restrizioni del prompt possono essere aggirate e raccomanda sanitizzazione, validazione, least privilege, separazione dei contenuti non attendibili e approvazione umana per operazioni ad alto rischio. [R7]

SEZIONE 3

Evidenze dalle policy ufficiali

Training, retention, revisione e funzioni stateful: cosa dichiarano i fornitori.

> **COME LEGGERE LA TABELLA**
> La tabella non assegna un “bollino privacy” ai marchi. Confronta configurazioni e categorie di servizio. Le condizioni cambiano e devono essere ricontrollate prima di ogni acquisto o rinnovo.

Soluzione	Training	Retention	Aspetti critici	Valutazione
ChatGPT consumer	Può utilizzare i contenuti per addestrare/migliorare i modelli, salvo opt-out; il feedback può includere l’intera conversazione.	Le chat eliminate sono rimosse entro 30 giorni con eccezioni; Temporary Chat entro 30 giorni.	Prompt, file, immagini, audio, video, servizi collegati e log.	Non adatto a dati non pubblici. [P1-P2]
Gemini Apps consumer	L’attività può essere usata per migliorare i modelli in base alle impostazioni.	Conversazioni già revisionate possono essere conservate fino a 3 anni anche dopo la disattivazione dell’attività.	Google dichiara revisione umana e invita a non inserire informazioni confidenziali.	Non adatto a dati non pubblici. [P4]
Claude consumer	Chat e sessioni di coding possono essere usate per migliorare Claude se l’utente sceglie di consentirlo; safety review, feedback e altri opt-in espliciti restano eccezioni.	Policy consumer e safety retention; trasferimenti e trattamento secondo l’informativa.	Input/output, feedback e informazioni tecniche.	Non adatto a dati non pubblici. [P5]
OpenAI API standard	No training per default sui prodotti business.	Abuse monitoring con contenuto fino a 30 giorni per impostazione standard; /v1/responses conserva application state per 30 giorni per default o con store=true; altre risorse stateful restano fino alla cancellazione.	ZDR/MAM soggetti ad approvazione e compatibilità di endpoint e modello; verificare Safety Retention, prompt caching, container e tool/MCP terzi.	Valutabile solo con gateway, endpoint verificati e retention controllata. [P3]
Anthropic API standard	I termini commerciali escludono il training sui Customer Content.	Per i modelli ordinari valgono eliminazione standard entro 30 giorni ed eccezioni documentate; i “Covered Models” designati richiedono 30 giorni di retention anche nei contesti ZDR.	ZDR solo per organizzazioni e prodotti eleggibili; classificatori di sicurezza, modello scelto e piattaforma di accesso richiedono una verifica separata.	Valutabile con DPA, modello e retention/ZDR documentati. [P6-P8, P12]
Microsoft Foundry / Azure	Prompt e output non usati per addestrare modelli senza autorizzazione.	Funzioni stateful conservano dati; abuse monitoring può prevedere storage/revisione.	Modified abuse monitoring può disabilitare storage/revisione; verificare ContentLogging.	Valutabile se configurata e verificata. [P9]
Google Cloud Gemini Enterprise Agent Platform	Nessun training/fine-tuning sui dati del cliente senza permesso.	Prompt logging, Advanced AI, grounding, session resumption e cache seguono regole distinte; per ZDR servono verifiche e configurazioni specifiche.	Search grounding conserva dati fino a 3 giorni; Maps fino a 30; session resumption fino a 24 ore. La cache in-memory ha TTL di 24 ore ed è dichiarata compatibile con ZDR, ma disattivabile.	Valutabile con endpoint e funzioni ZDR compatibili. [P10]
Gemini Developer API (Paid)	No training per migliorare i prodotti; prompt e risposte trattati secondo DPA.	Logging limitato per abuso; ZDR solo dopo approvazione del progetto. Grounding Search/Maps: 30 giorni.	Interactions: store=false; Live, Files e cached_content hanno retention propria; client non accessibili a minori di 18 anni.	Valutabile solo con Paid Services, DPA, ZDR attivo e funzioni compatibili. [P14-P15]
Amazon Bedrock	AWS non usa input/output per addestrare i modelli; il trattamento del model provider dipende dalla modalità di retention e dai termini del modello.	La retention dipende dal modello e dalla modalità default, none o provider_data_share; store=false, da solo, non garantisce ZDR.	In modalità none non vi è storage durevole né condivisione; provider_data_share consente retention e condivisione per i modelli che la richiedono.	Valutabile solo verificando allowed_modes, modello, regione, logging cliente e policy effettiva. [P11, P13]
IA locale / self-hosted	Nessun training del provider perché non avviene una chiamata esterna.	Retention decisa dall’organizzazione: può essere zero per contenuto e limitata per metadati.	Rischio di telemetria, log, backup, accessi interni e supply chain.	Preferibile per dati ad alta sensibilità, con hardening.

3.1 La prova più chiara: i provider distinguono consumer e business/API

OpenAI precisa che la privacy policy consumer non si applica ai contenuti trattati per i clienti business/API e che, per i prodotti business, input e output non sono usati per training per default. Anthropic separa i servizi consumer da quelli commerciali e nei termini commerciali dichiara che non può addestrare modelli sul Customer Content. Questa separazione conferma che l'architettura e il contratto contano almeno quanto il nome del modello. [P1-P3, P5-P6]

3.2 API: eccezioni che devono entrare nel capitolato

La documentazione OpenAI mostra che Chat Completions e Responses non sono usate per training, ma in configurazione standard generano abuse monitoring fino a 30 giorni. /v1/responses conserva application state per 30 giorni per default o con store=true; Conversations, ChatKit, Assistants, Threads, vector store e file seguono cicli distinti e non sono tutti eleggibili per ZDR. Prompt caching può conservare tensori cifrati su GPU fino a 24 ore; tool/MCP terzi seguono le proprie policy; Safety Retention può introdurre eccezioni comunicate al cliente. Non basta quindi scegliere "OpenAI API": occorre specificare endpoint, parametri, modello, funzioni vietate e prova della configurazione ZDR/MAM. [P3]

Anthropic dichiara cancellazione standard entro 30 giorni per l'API, con eccezioni per Files API, enforcement, accordi e legge. Lo ZDR è soggetto ad approvazione e copre solo organizzazioni e prodotti eleggibili; restano alcuni risultati dei classificatori di sicurezza. Dal 9 giugno 2026, inoltre, i "Covered Models" designati richiedono 30 giorni di retention di prompt e output anche quando l'accesso avviene in contesti ZDR, compresi i cloud partner. [P7-P8, P12]

Google richiede una distinzione ulteriore. Nel Gemini Developer API, i Paid Services escludono l'uso di prompt e risposte per migliorare i prodotti e li sottopongono al DPA; resta tuttavia il logging limitato per l'abuse monitoring finché la richiesta ZDR non è approvata per lo specifico progetto. Dopo l'approvazione, Google dichiara la rimozione di contenuti e metadati identificabili prima del logging. Grounding con Search e Maps conserva contenuti per 30 giorni; l'Interactions API richiede store=false per evitare lo stato persistente; Live session resumption, File API e cached_content hanno cicli separati. I termini vietano inoltre client API diretti o verosimilmente accessibili a minori di 18 anni, un vincolo contrattuale distinto dal GDPR. Queste regole non vanno confuse con Gemini Enterprise Agent Platform, dove il Search grounding può conservare dati fino a 3 giorni e altre funzioni seguono condizioni diverse. Microsoft e AWS confermano lo stesso principio generale: core inference no-training non esclude abuse monitoring, funzioni stateful o regole del singolo modello. In Bedrock, store=false non garantisce ZDR: servono la modalità effettiva e gli allowed_modes. [P9-P11, P13-P15]

3.3 "No-training" è necessario ma non sufficiente

Domanda	Evidenza richiesta
Il contenuto addestra il modello?	Clausola no-training per input, output, allegati e feedback; opt-in solo con autorizzazione.
Il contenuto viene registrato?	Tabella di retention per endpoint e funzione; distinzione tra abuse log e application state.
Chi può leggerlo?	Regole di human review, ruoli autorizzati, escalation e tracciamento degli accessi.
Dove viene processato?	Regione/data zone, trasferimenti, subprocessori, SCC e servizi globali.
Cosa succede ai file?	Ciclo di vita, cancellazione automatica, vector store, cache, backup e test di cancellazione.
Cosa registriamo noi?	Configurazione di reverse proxy, APM, error tracking, tracing, database e queue.
Le funzioni esterne hanno altre policy?	Elenco connettori/tool/MCP e divieto di invio a terzi non approvati.

SEZIONE 4

Quadro GDPR e responsabilità

Il titolare deve dimostrare perché il trattamento è necessario, proporzionato e sicuro.

4.1 Principi applicabili

Riferimento	Implicazione per chatbot e API
Art. 5	Finalità, minimizzazione, esattezza, limitazione della conservazione, integrità/riservatezza e accountability. Un prompt deve contenere solo ciò che serve.
Art. 6	Ogni trattamento richiede una base giuridica. Un account personale non crea una base per inviare dati di terzi.
Art. 9	Dati sanitari, disabilità, convinzioni, biometria e altre categorie particolari richiedono condizioni rafforzate e tutele elevate.
Art. 25	Privacy by design e by default: la configurazione più protettiva deve essere incorporata nell'architettura.
Art. 28	Il fornitore che tratta dati per conto dell'ente deve essere disciplinato da un DPA con istruzioni, sicurezza, subprocessori, cancellazione e assistenza.
Art. 32	Misure tecniche e organizzative adeguate: controllo accessi, cifratura, resilienza, test, incident response e gestione dei segreti.
Art. 35	DPIA quando, considerate nuove tecnologie, natura, ambito, contesto e finalità, il trattamento può presentare un rischio elevato per i diritti e le libertà; soglia di cautela particolarmente alta con minori o dati particolari.
Artt. 44-49	Individuare dove avvengono processing, storage, supporto e revisione e le garanzie per i trasferimenti internazionali.

[R1] Regolamento (UE) 2016/679, testo ufficiale EUR-Lex.

4.2 DPIA, DPO e riferimenti per la scuola

Le Guidance EDPS sulla generative AI sono rivolte direttamente alle istituzioni e agli organi dell'Unione soggetti al regolamento (UE) 2018/1725; in questo dossier sono usate come autorevole riferimento interpretativo, non come fonte direttamente vincolante per le scuole italiane. Per queste ultime il quadro applicabile resta fondato su GDPR, normativa nazionale e provvedimenti del Garante. [R2]

Nel parere del 4 agosto 2025 sulle Linee guida MIM, il Garante ha richiamato, tra le garanzie recepite nello schema, l'uso dei dati personali di studenti e docenti solo quando strettamente indispensabile, il ricorso ove possibile a dati sintetici, configurazioni che impediscano la conservazione dei prompt, la profilazione o il tracciamento, formazione, audit periodici e valutazione d'impatto. La richiesta di informazioni del 3 giugno 2026 al Centro Nazionale Opere Salesiane Scuola non accerta una violazione, ma conferma l'attenzione dell'Autorità su provider, flussi di dati e DPIA. [R8-R9]

GDPR e AI Act operano in parallelo. Il Regolamento (UE) 2024/1689 è applicabile in via generale dal 2 agosto 2026 e le regole di trasparenza decorrono da agosto 2026; dopo l'AI Omnibus, le regole per i sistemi ad alto rischio in settori tra cui l'istruzione si applicano dal 2 dicembre 2027 e quelle per i sistemi incorporati in prodotti regolamentati dal 2 agosto 2028. Questa scansione non sospende gli obblighi GDPR già applicabili. [R10-R11]

La DPIA non è un modulo da compilare dopo il rilascio. Deve descrivere flussi di dati, categorie e interessati, necessità e proporzionalità, provider e subprocessori, retention, controlli tecnici, rischio residuo, test e gestione degli incidenti. Per un chatbot scolastico con dati di minori o documenti individuali, la soglia di cautela è elevata.

4.3 Ruoli e accountability

Ruolo	Responsabilità minima
Vertice / titolare	Approvare finalità, classi di dati ammesse, budget, responsabilità e rischio residuo.

Ruolo	Responsabilità minima
DPO	Fornire consulenza su liceità, DPIA, DPA, trasferimenti e diritti degli interessati; sorvegliare la conformità senza sostituirsi al titolare.
CISO / IT	Progettare gateway, IAM, egress, logging, cifratura, segregazione, patching e monitoraggio.
Ufficio acquisti/legale	Inserire clausole su no-training, retention, subprocessori, incidenti, audit, cancellazione e recesso.
Responsabile applicativo	Definire use case, dataset, endpoint, test, human review e qualità degli output.
Utente	Rispettare la classificazione, non aggirare i controlli, segnalare errori e incidenti.

> **!** **ERRORE DI GOVERNANCE**
> Affidare la conformità alla prudenza individuale ("non incollare dati sensibili") è insufficiente. La privacy by default richiede che l'interfaccia impedisca o riduca tecnicamente l'invio, e che le eccezioni siano autorizzate e tracciate.

SEZIONE 5

Architetture raccomandate

API-first per l'uso ordinario; local-first per i dati più sensibili.

5.1 Gateway API con retention controllata

Architettura raccomandata: API attraverso un gateway organizzativo

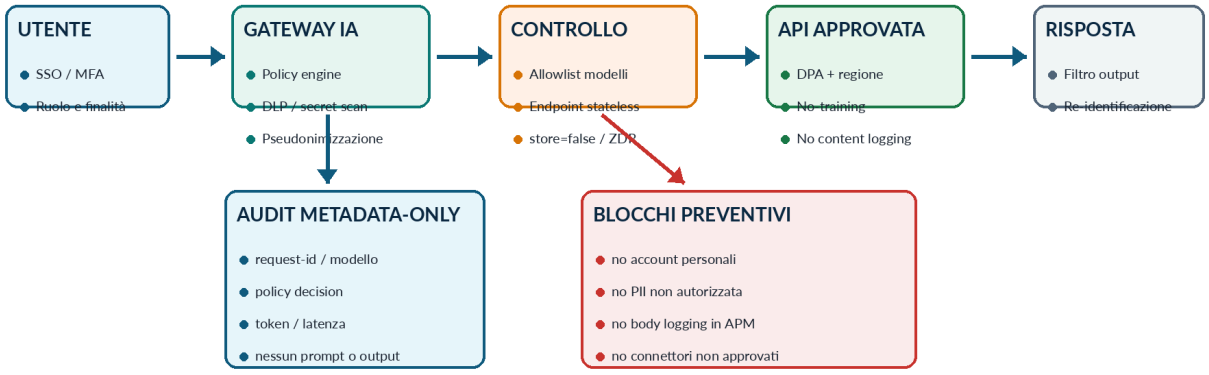

Figura 2 - Il provider è un componente dietro controlli organizzativi.

Il gateway deve essere il solo componente autorizzato a conoscere le chiavi del provider. Gli utenti non ricevono API key e non possono selezionare liberamente endpoint o connettori. Il flusso consigliato è:

1. Autenticazione SSO/MFA e autorizzazione per ruolo, struttura e finalità.
2. Classificazione del caso d'uso e del dato; blocco immediato delle categorie vietate.
3. DLP, secret scanning, rimozione di identificativi e pseudonimizzazione prima della chiamata.
4. Selezione da allowlist di provider, modello, regione, endpoint e parametri compatibili con la retention approvata.
5. Chiamata stateless con storage disabilitato; ZDR/no content logging verificati dove richiesti.
6. Filtro dell'output per PII, segreti, contenuto non autorizzato e prompt leakage.
7. Re-identificazione soltanto nell'applicazione interna e solo per gli utenti autorizzati.
8. Audit metadata-only con retention breve; nessun prompt o output nei log ordinari.

5.2 Requisiti tecnici del gateway

Dominio	Controllo minimo
Identità	OIDC/SAML, MFA, RBAC/ABAC, service account separati, rotazione delle chiavi.
Data minimization	Template di prompt, campi strutturati, pseudonimi, redazione, tokenizzazione e synthetic data.
Provider policy	Adapter per provider che impone endpoint, regione, store=false e funzioni consentite.
Logging	Disabilitare body logging; filtri in reverse proxy, APM, error tracker, Celery, queue e database.
Stateful storage	Vietato per default; se indispensabile, TTL, cifratura, ownership, job di cancellazione e test.
Connettori	Disabilitati per default; ogni tool ha identità minima, allowlist e revisione della propria privacy policy.
Output security	Validazione schema, DLP, escaping, controllo di comandi/tool call e human approval.
Observability	Metriche senza contenuto: latenza, token, errori, modello, policy decision, request hash.
Incident response	Kill switch, revoca chiavi, quarantena, export audit e notifica DPO/CISO.

5.3 IA locale / on-premise

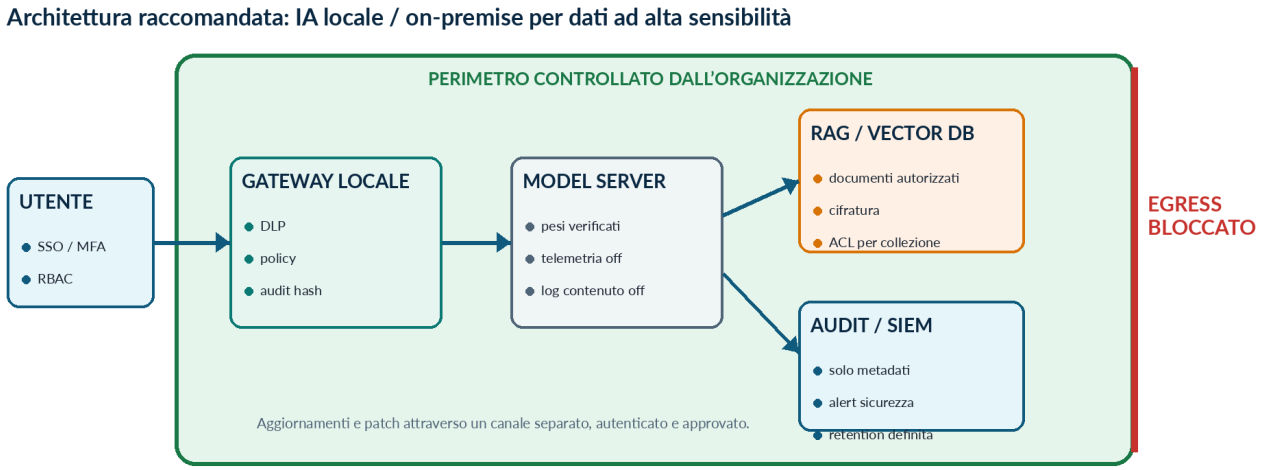

Figura 3 - Il contenuto resta nel perimetro, ma il perimetro deve essere realmente chiuso e gestito.

Nel modello prudenziale proposto, l'IA locale è preferibile quando il danno derivante dalla divulgazione è elevato o quando il trattamento riguarda categorie particolari, minori, segreti o dossier individuali. L'obiettivo non è costruire un "chatbot senza regole", ma mantenere inferenza, RAG e storage sotto il controllo dell'organizzazione.

- Egress negato al runtime; gli aggiornamenti passano da un canale separato, autenticato e approvato.
- Telemetria, crash dump, analytics e invio automatico di prompt disattivati e verificati con network monitoring.
- Pesi e container acquisiti da fonti autorizzate, con hash/firme, SBOM e vulnerability scanning.
- Model server senza request/response logging; system log separati e sanitizzati.
- Vector database cifrato, con ACL per collezione e retrieval limitato al ruolo dell'utente.
- Documenti RAG classificati, versionati e sottoposti a retention; nessun accesso indiscriminato a file share.
- Backup cifrati e separati, con ciclo di cancellazione coerente con l'applicazione.
- Human-in-the-loop per decisioni o documenti con effetti sulle persone.

5.4 Quando una API è preferibile al locale

Il locale non è sempre la scelta migliore. Una API cloud ben contrattualizzata può offrire modelli più capaci, patch rapide, compliance certificata e minore onere operativo. È preferibile quando i dati possono essere minimizzati o pseudonimizzati, il provider offre retention adeguata, la regione è accettabile e il rischio residuo è più basso rispetto a un'infrastruttura locale non gestita.

La scelta corretta confronta il rischio del trasferimento a terzi con il rischio operativo interno. L'organizzazione deve dimostrare perché l'architettura selezionata è adeguata allo specifico caso d'uso.

SEZIONE 6

Matrice decisionale per i dati

La matrice C0-C3 è un modello interno di classificazione del rischio, non una tassonomia prevista dal GDPR o dall'AI Act e non sostituisce base giuridica, DPIA o valutazione del caso concreto. La soluzione dipende dalla sensibilità e dalla finalità del trattamento, non dalla comodità dell'utente.

Classe	Esempi	Canale raccomandato	Condizioni
C0 - Pubblico	Norme pubblicate, materiale promozionale, testi già online, dati sintetici.	Consumer valutabile con cautela; API o locale valutabili secondo finalità, policy, configurazione e misure applicabili.	Nessuna credenziale, dato nascosto o metadato non pubblico.
C1 - Interno	Procedure, bozze generiche, appunti senza PII, codice non segreto.	SaaS enterprise o API controllata; consumer sconsigliato.	No-training, accessi organizzativi, log di contenuto disattivati.
C2 - Riservato	Contratti, codice proprietario, dati cliente pseudonimizzati, documenti non pubblici.	API con DPA, ZDR/retention minima e DLP; locale preferibile.	DPIA/valutazione, regione, no connettori, audit metadata-only.
C3 - Limitato	Dati sanitari, minori, PEI/PDP, HR/disciplinare, contenzioso, credenziali, segreti.	Locale/on-prem di default; API solo con autorizzazione formale e garanzie rafforzate.	Pseudonimizzazione, egress control, least privilege, human review.

6.1 Scuola

Nel contesto scolastico, la combinazione di minori, dati sanitari, disabilità, BES/DSA, valutazioni e relazioni familiari rende particolarmente pericolosa la copia di documenti in una chat pubblica. Devono essere considerati C3 almeno:

- PEI, PDP, diagnosi, certificazioni, verbali GLO, relazioni di sostegno e documenti dei servizi sociali;
- nomi associati a voti, note disciplinari, assenze, comportamenti, fragilità o bisogni educativi;
- registrazioni audio/video, fotografie, elaborati identificabili e comunicazioni scuola-famiglia;
- dati del personale, procedimenti, malattia, permessi, contenzioso e documentazione sindacale;
- credenziali, token, esportazioni dal registro elettronico e archivi amministrativi.

✓ **ESEMPIO SICURO**

Per generare una bozza didattica si può usare un profilo sintetico ("studente A, classe seconda, difficoltà di lettura") senza nome, diagnosi, scuola, famiglia o dettagli univoci. Per lavorare sul documento reale occorre un ambiente locale o un percorso API formalmente autorizzato.

6.2 Pubblica amministrazione

La PA deve evitare che istanze, protocolli, dati tributari, anagrafici, sanitari, giudiziari o di vulnerabilità finiscano in servizi consumer. Anche la semplice richiesta può rivelare informazioni: il ruolo dell'utente, la data e il contesto di una domanda possono avere valore sensibile. L'uso ammesso deve passare da strumenti istituzionali, con DPA, registro dei trattamenti, controllo dei fornitori e audit.

6.3 Impresa e professioni

Sono ad alto rischio codice sorgente, roadmap, contratti, listini non pubblici, credenziali, dati clienti, M&A, brevetti, strategie, documenti legali e HR. L'API controllata permette di automatizzare classificazione, riepilogo, traduzione e drafting senza consegnare agli utenti le chiavi e senza registrare il contenuto nei log; i segreti più critici restano su un modello locale o in un private cloud isolato.

SEZIONE 7

Capitolato, policy e controlli verificabili

Le garanzie devono diventare requisiti contrattuali e test tecnici.

7.1 Checklist per il fornitore

- DPA conforme all'art. 28 e chiara qualificazione dei ruoli.
- Divieto di training o miglioramento su input, output, allegati, embeddings e feedback, salvo opt-in scritto.
- Retention per endpoint e funzione, con elenco delle eccezioni; ZDR/no content logging dove richiesto.
- Procedura e prova tecnica per verificare la configurazione effettiva.
- Elenco subprocessori, localizzazione, trasferimenti e meccanismi ex artt. 44-49 GDPR.
- Cancellazione di file, thread, vector store, cache, backup e dati alla cessazione.
- Regole di human review, accessi privilegiati e registrazione degli accessi al contenuto.
- Notifica degli incidenti, tempi, collaborazione forense e disponibilità dei log di sicurezza.
- Cifratura in transito e a riposo, gestione chiavi, private connectivity e segregazione dei tenant.
- Portabilità, export, exit plan e distruzione dei dati alla fine del contratto.
- Clausole su preview/beta: vietate per dati reali salvo nuova valutazione.
- Diritto di audit, attestazioni indipendenti e documentazione tecnica aggiornata.

7.2 Clausole tecniche da non confondere

Clausola	Che cosa garantisce	Che cosa NON garantisce
No-training	Il contenuto cliente non alimenta l'addestramento/miglioramento del modello.	Non elimina abuse log, storage stateful, backup o revisione.
Zero Data Retention	Il provider non conserva il contenuto per gli endpoint eleggibili, salvo eccezioni definite.	Non impedisce alla nostra app o a un connettore di registrare i dati.
Data residency	Storage/processing in una regione o data zone definita.	Non equivale automaticamente a nessun trasferimento o accesso remoto.
Encryption	Riduce l'esposizione a riposo/in transito.	Il servizio deve comunque decifrare i dati per elaborarli, salvo tecniche speciali.
Private endpoint	Evita il transito sulla rete Internet pubblica.	Non elimina retention, training o log applicativi.
Enterprise plan	Aggiunge governance e contratto.	Non rende leciti tutti i dati e tutte le finalità.

7.3 Policy interna: dieci regole non negoziabili

1. È vietato inserire dati C2/C3 in chatbot consumer o account personali.
2. Si usano esclusivamente strumenti approvati e accessibili con identità organizzativa.
3. Ogni caso d'uso ha un owner, una finalità documentata e una classe di dati ammessa.
4. I dati vengono minimizzati e pseudonimizzati prima dell'invio.
5. API key e credenziali restano nel backend; mai nel browser, nel client o nel prompt.
6. Prompt e output non vengono salvati nei log, nei ticket o nei sistemi APM.
7. File, thread e vector store hanno TTL e cancellazione automatica verificata.
8. Connettori, web search e tool sono disattivati per default e autorizzati singolarmente.
9. Gli output sono sempre revisionati da una persona per atti, valutazioni o decisioni.
10. Ogni incidente o invio errato viene segnalato immediatamente a IT/DPO/CISO.

SEZIONE 8

Piano operativo 30-60-90 giorni

Dalla ricerca a una governance verificabile.

Fase	Azioni	Risultato atteso
0-30 giorni	Inventario strumenti e account; blocco chatbot consumer per C2/C3; policy provvisoria; mappatura use case; coinvolgimento DPO/CISO.	Riduzione immediata dello shadow AI e visibilità sul rischio.
31-60 giorni	Selezione provider/API; DPA e requisiti retention; prototipo gateway con SSO, DLP, no body logging; classificazione dati; DPIA prioritarie.	Canale istituzionale controllato per i casi ordinari.
61-90 giorni	Pilota locale per C3; test di egress e telemetria; cancellazione file/vector store; penetration/prompt injection test; formazione e metriche.	Architettura differenziata API/local e controlli dimostrabili.
Continuativo	Riesame trimestrale policy e provider; test di configurazione; audit accessi; tabletop incident; aggiornamento DPIA e subprocessori.	Accountability e adattamento alle condizioni che cambiano.

8.1 Test di accettazione prima del go-live

- Inviare un identificatore fittizio e verificare che venga redatto prima della API call.
- Generare un errore e controllare che prompt e risposta non compaiano in proxy, APM, Sentry, Celery, database o console.
- Creare e cancellare un file/vector store, verificando API, dashboard e job di retention.
- Verificare la configurazione ZDR/no content logging con prova esportabile o screenshot amministrativo.
- Tentare di usare un endpoint o connettore non allowlisted: la richiesta deve essere bloccata.
- Inserire una prompt injection in un documento RAG e verificare che non possa estrarre altri documenti o invocare tool.
- Sul locale, osservare il traffico di rete durante inferenza e crash: nessun egress non autorizzato.
- Verificare RBAC: un utente non deve recuperare embeddings o documenti di un'altra collezione.
- Testare kill switch, revoca chiavi, cancellazione e procedura di incidente.

8.2 Indicatori utili

Indicatore	Misurazione
Adozione controllata	Quota di richieste IA effettuata dal gateway rispetto agli strumenti non approvati.
Minimizzazione	Percentuale di richieste bloccate/redatte dal DLP per classe di dato.
Retention	Numero di oggetti stateful oltre TTL; deve tendere a zero.
Logging	Esiti del test periodico di assenza prompt/output nei sistemi osservabili.
Governance	Use case con owner, valutazione e DPIA/DPA completati.
Sicurezza	Prompt injection test, incidenti, tempo di revoca e copertura patch.

CONCLUSIONI

La scelta raccomandata

Controllare il flusso dei dati prima di scegliere il modello.

Le fonti ufficiali dei provider confermano che le modalità consumer possono comprendere training, retention, revisione umana, dati dei servizi collegati e trasferimenti. Le stesse fonti confermano anche che le offerte business e API possono prevedere no-training, retention limitata, ZDR, regioni e controlli amministrativi. La conclusione corretta non è "il cloud è sempre illecito", ma "la chat pubblica è inadeguata ai dati non pubblici e il cloud deve essere reso controllabile attraverso contratto, configurazione e architettura".

L'API è il punto di equilibrio per molti casi: consente di ridurre il dato prima dell'invio, imporre endpoint e provider approvati, disattivare lo storage, evitare log di contenuto e mantenere un audit minimo. Tuttavia, la zero retention deve essere provata per ogni funzione, e l'applicazione cliente deve essere progettata per non ricreare la traccia che si voleva evitare.

L'IA locale è preferibile per i dati più sensibili perché può eliminare la trasmissione a un terzo. Questa proprietà esiste soltanto se il runtime è realmente isolato, la telemetria è spenta, il RAG è segregato, i log non contengono dati e l'organizzazione è in grado di mantenere la piattaforma.

✓ **DECISIONE FINALE**

Vietare i chatbot consumer per dati non pubblici. Istituire un gateway API con DPA, no-training, retention minima/ZDR, DLP e logging metadata-only. Riservare IA locale/on-premise ai dati C3 e ai casi in cui sovranità, segreto o impatto sugli interessati rendono inaccettabile la trasmissione a un provider.

Regola finale per modello

Modello	Uso raccomandato	Condizioni indispensabili
Chatbot consumer	Solo dati C0 già pubblici o contenuti sintetici.	Nessun dato personale di terzi, segreto, credenziale, documento interno o metadato non pubblico.
API controllata	Default per C1 e C2 e per automazioni organizzative ordinarie.	DPA, no-training, retention minima/ZDR verificata, minimizzazione, DLP, endpoint allowlist e no content logging.
IA locale / privata	Default per C3 e per casi in cui la trasmissione a terzi è inaccettabile.	Egress e telemetria bloccati, log di contenuto disattivati, RAG segregato, hardening, patching e backup controllati.

APPENDICE A

Specifiche minime per un gateway IA

Requisiti implementativi traducibili in backlog e criteri di collaudo.

Componente	Specifiche
Input schema	Campi strutturati; lunghezza e MIME limitati; nessun upload arbitrario.
PII/secret detector	Regex + NER + dizionari organizzativi; blocco o redazione; eccezione approvata.
Pseudonym vault	Mappaggio identificatori custodito internamente; provider riceve token casuali, non identità.
Provider adapter	Configurazione immutabile per modello/endpoint/region/store/tools; nessun parametro utente libero.
Request context	Finalità e classe di dato firmate dal policy engine; non inserite nel prompt se contengono PII.
Content logging	Body disabilitato su web server, ingress, API gateway, APM, tracing, error tracking e queue.
Audit record	ID utente/ruolo, timestamp, use case, provider/modello, token, policy decision, hash; TTL definito.
Response filter	Schema validation, PII scan, tool-call allowlist, citation/provenance quando richiesta.
Storage lifecycle	Default stateless; TTL automatico per file/vector store; cancellazione su richiesta/cessazione.
Feature flags	Web search, connector, MCP, code interpreter, memory e background jobs off di default.
Key management	Secret manager/KMS, rotazione, scoped key per ambiente, mai log o client-side.
Network	TLS; private endpoint quando disponibile; egress allowlist; DNS e proxy monitorati.
Resilience	Timeout, circuit breaker, rate limit, budget, fallback che non riduce la protezione.
Security testing	SAST/DAST, dependency scanning, prompt injection, data exfiltration e tenant isolation.

Esempio di record di audit ammesso

```
request_id=7f...  user_role=docente  use_case=bozza_didattica  data_class=C1
provider=azure  model=approved-model-v3  input_tokens=542  output_tokens=388
policy=ALLOW_REDACTED  pii_redactions=2  stateful=false  content_logged=false  ttl_days=30
```

Non devono essere inclusi prompt, risposta, allegati, nomi, email, token di autenticazione o stack trace contenenti il body della richiesta.

APPENDICE B

Fonti primarie e documentazione

Fonti ricontrollate il 27 luglio 2026. Verificare nuovamente policy, contratto e configurazione prima della pubblicazione, dell'acquisto o del go-live.

[R1] Unione europea - Regolamento (UE) 2016/679 (GDPR), EUR-Lex. Apri la fonte

[R2] European Data Protection Supervisor - Guidance on generative AI and data protection for EU institutions, revised 28 ottobre 2025. Apri la fonte

[R3] European Data Protection Board - Opinion 28/2024 on certain data protection aspects related to AI models, 18 dicembre 2024. Apri la fonte

[R4] NIST - Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, NIST AI 600-1, 2024. Apri la fonte

[R5] UK National Cyber Security Centre - ChatGPT and LLMs: what's the risk. Apri la fonte

[R6] OWASP GenAI Security Project - LLM02:2025 Sensitive Information Disclosure. Apri la fonte

[R7] OWASP GenAI Security Project - LLM01:2025 Prompt Injection. Apri la fonte

[R8] Garante per la protezione dei dati personali - Parere sulle Linee guida MIM per l'IA nelle istituzioni scolastiche, 4 agosto 2025. Apri la fonte

[R9] Garante per la protezione dei dati personali - IA a scuola: richiesta di informazioni agli istituti Salesiani, 3 giugno 2026. Apri la fonte

[R10] Unione europea - Regolamento (UE) 2024/1689 (AI Act), EUR-Lex. Apri la fonte

[R11] Commissione europea - AI Act: quadro e calendario di applicazione aggiornato dopo l'AI Omnibus. Apri la fonte

[P1] OpenAI - Europe Privacy Policy, aggiornata 4 giugno 2026. Apri la fonte

[P2] OpenAI Help Center - How your data is used to improve model performance. Apri la fonte

[P3] OpenAI Developers - Data controls in the OpenAI platform. Apri la fonte

[P4] Google - Gemini Apps Privacy Hub. Apri la fonte

[P5] Anthropic Privacy Center - Is my data used for model training? Apri la fonte

[P6] Anthropic - Commercial Terms of Service. Apri la fonte

[P7] Anthropic Privacy Center - How long do you store my organization's data? Apri la fonte

[P8] Anthropic Privacy Center - Zero data retention: eligible products and limitations. Apri la fonte

[P9] Microsoft Learn - Data, privacy, and security for Models sold by Azure in Microsoft Foundry. Apri la fonte

[P10] Google Cloud - Gemini Enterprise Agent Platform and zero data retention. Apri la fonte

[P11] Amazon Web Services - Data protection in Amazon Bedrock. Apri la fonte

[P12] Anthropic Privacy Center - Data retention practices for Covered Models. Apri la fonte

[P13] Amazon Web Services - Data retention in Amazon Bedrock. Apri la fonte

[P14] Google AI for Developers - Zero data retention in the Gemini Developer API. Apri la fonte

[P15] Google AI for Developers - Gemini API Additional Terms of Service. Apri la fonte

i	**NOTA DI VALIDITÀ** Questo documento è informativo e tecnico-organizzativo; non sostituisce un parere legale sul singolo trattamento. Policy, prodotti e opzioni di retention cambiano rapidamente: verificare sempre contratto, DPA, documentazione dell'endpoint e configurazione effettiva prima del go-live.

ORIZZONTE INSEGNANTI

Governare l'IA significa governare il percorso dei dati.

Dossier aggiornato al 27 luglio 2026

REGISTRO DI VERIFICA — 27 LUGLIO 2026

Sintesi delle verifiche

Le verifiche sulle fonti primarie effettuate il 27 luglio 2026 sono già incorporate nel corpo del dossier. Questo registro documenta le variazioni sostanziali e consente di distinguere i dati rimasti confermati dalle correzioni rese necessarie dall'evoluzione delle policy e del quadro europeo.

Modifiche integrate nel corpo

1. OpenAI. Per l'API restano confermati no-training per default e abuse monitoring fino a 30 giorni nella configurazione standard. Sono ora esplicitati anche i 30 giorni di application state predefinito di /v1/responses, la cache di prompt fino a 24 ore, le policy proprie dei tool/MCP terzi e le possibili eccezioni di Safety Retention. [P3]

2. Google Gemini consumer. Con Keep Activity disattivato, le chat future non sono usate per il training salvo feedback e sono conservate per 72 ore; le conversazioni già revisionate possono restare fino a tre anni, disconnesse dall'account. [P4]

3. Anthropic. Le regole standard di retention e ZDR sono confermate, ma dal 9 giugno 2026 i "Covered Models" designati richiedono 30 giorni di retention di prompt e output anche nei contesti ZDR e tramite cloud partner. Modello e piattaforma devono quindi essere verificati insieme. [P7-P8, P12]

4. Google Cloud Gemini Enterprise Agent Platform. Grounding con Google Search conserva dati fino a 3 giorni, non 30; Maps arriva a 30 giorni. Session resumption arriva a 24 ore. La cache in-memory ha TTL di 24 ore ed è dichiarata compatibile con ZDR, pur essendo disattivabile. [P10]

5. Microsoft Foundry/Azure. Sono confermati no-training senza autorizzazione, controlli distinti per abuse monitoring e la necessità di verificare l'effettiva approvazione al modified abuse monitoring e il valore ContentLogging=false. [P9]

6. Amazon Bedrock. Non è più corretta una descrizione assoluta di assenza di storage o condivisione. La retention dipende dalla modalità effettiva e dagli allowed_modes del modello: none impedisce storage durevole e condivisione, provider_data_share li consente per i modelli che lo richiedono e store=false, da solo, non garantisce ZDR. [P11, P13]

7. Quadro italiano ed europeo. Sono stati integrati il parere del Garante sulle Linee guida MIM, la richiesta di informazioni del 3 giugno 2026, il corretto ambito delle Guidance EDPS e il calendario aggiornato dell'AI Act: applicazione generale dal 2 agosto 2026, trasparenza da agosto 2026, sistemi ad alto rischio in settori tra cui l'istruzione dal 2 dicembre 2027 e sistemi incorporati in prodotti regolamentati dal 2 agosto 2028. [R2, R8-R11]

8. Gemini Developer API. È stata introdotta la distinzione tra Paid Services, esclusione dell'uso per migliorare i prodotti, DPA e ZDR di progetto; sono esplicitati i 30 giorni di retention per Grounding con Search e Maps, store=false per Interactions, i cicli separati di Live, Files e cache e il limite contrattuale per client diretti o verosimilmente accessibili a minori di 18 anni. [P14-P15]

Nota editoriale

Il dossier è informativo e tecnico-organizzativo e non costituisce consulenza legale. Prima di acquisto, rinnovo o uso con dati personali occorre ricontrollare contratto, DPA, subprocessori, regione, modello, endpoint, parametri, funzioni attive e configurazione effettiva del tenant o del progetto.