QUADRO SINOTTICO – COMPLIANCE NIS2/GDPR/AI ACT: PROVIDER AI

Gruppo ICT CRUI

Rev. giugno 2026 (aggiornamento da rev. marzo 2026)

Questo aggiornamento include una sezione AI Act.

La valutazione è condotta ai fini della compliance con la Direttiva NIS2 (D.Lgs. 138/2024), il GDPR (Reg. UE 2016/679) e il Regolamento AI (Reg. UE 2024/1689), con particolare riferimento ai requisiti di sicurezza della catena di approvvigionamento e alla qualificazione ACN ai sensi del Regolamento ACN n. 21007/2024.

Perimetro: account enterprise / API dei provider (piano consumer escluso dal perimetro d'uso istituzionale).

Stato della cella: ■ Conforme/Disponibile ■ Parziale/Condizionato ■ Non disponibile/Non dichiarato

Tipo di fonte:

✓ **Verificato** = fonte primaria letta in questa revisione

Dichiarato dal fornitore = affermazione del fornitore non verificata da terzi

Certificazioni dichiarate : report richiedibili = report disponibile su richiesta tramite Trust Center/NDA

⚠ **Da verificare** = fonte non letta in questa revisione

Ambito di valutazione	OpenAI (ChatGPT Ent./API)	Google (Gemini / Vertex AI)	Microsoft (Azure OpenAI)	Anthropic (Claude Ent./API)
1. Qualificazione ACN e Certificazioni				
Catalogo ACN: https://www.acn.gov.it/portale/catalogo-delle-infrastrutture-digitali-e-dei-servizi-cloud				
1.1 Qualificazione ACN infrastruttura cloud	**Non qualificata** ✓ **Verificato** *OpenAI non risulta nel Catalogo ACN. L'eventuale uso tramite Azure OpenAI richiede verifica della specifica scheda ACN, del servizio, della regione, del modello contrattuale e delle componenti effettivamente adottate. La qualificazione dell'infrastruttura/CSP non equivale automaticamente a qualificazione del servizio AI specifico.* **Fonte:** *acn.gov.it/portale/catalogo-delle-infrastrutture-digitali-e-dei-servizi-cloud* ⚠ **Da verificare** *Stato eventuale iter qualificazione OpenAI: non trovato su fonte ufficiale.* **Verificare su:** *acn.gov.it*	**Livello 2 (QC2/QI2)** ✓ **Verificato** *Google Cloud presente nel Catalogo ACN con qualifica livello 2. La qualificazione riguarda singole schede/servizi: verificare le schede specifiche dei servizi adottati.* **Fonte:** *acn.gov.it/portale/catalogo-delle-infrastrutture-digitali-e-dei-servizi-cloud*	**Qualificata nel Catalogo ACN (servizi Microsoft Azure)** ✓ **Verificato** *La qualificazione riguarda le specifiche schede di servizio (IaaS/PaaS/SaaS) presenti nel Catalogo ACN. L'eventuale utilizzo tramite Polo Strategico Nazionale costituisce un distinto modello di erogazione e non rappresenta il presupposto della qualificazione ACN del servizio.* **Fonte:** *acn.gov.it/portale/catalogo-delle-infrastrutture-digitali-e-dei-servizi-cloud*	**Non qualificata** ✓ **Verificato** *Anthropic non risulta nel Catalogo ACN (giugno 2026). La qualifica del layer CSP (AWS/Azure) non si estende al servizio AI di Anthropic.* **Fonte:** *acn.gov.it/portale/catalogo-delle-infrastrutture-digitali-e-dei-servizi-cloud*
1.2 ISO/IEC 27001 Certificazioni	**Certificazioni e attestazioni disponibili** **Certificazioni dichiarate (report richiedibili)** *SOC 2 Type II* *ISO 27001* *ISO 27017* *ISO 27018* *ISO 27701.* *Report richiedibili tramite trust.openai.com.* **Fonte dichiarazione:** *openai.com/security-and-privacy (letta giugno 2026)*	**Certificazioni e attestazioni disponibili** **Certificazioni dichiarate (report richiedibili)** *ISO 27001* *ISO 27017* *ISO 27018* *ISO 27701* *SOC 1/2/3* *FedRAMP High.* **Fonte dichiarazione:** *cloud.google.com/security/compliance* ✓ **Verificato**	**Certificazioni e attestazioni disponibili** **Certificazioni dichiarate (report richiedibili)** • *ISO/IEC 27001* • *ISO/IEC 27017* • *ISO/IEC 27018* • *SOC 1* • *SOC 2* • *FedRAMP (per i servizi inclusi nel relativo programma)* • *HIPAA Business Associate Agreement (BAA) disponibile*	**Certificazioni e attestazioni disponibili** **Certificazioni dichiarate (report richiedibili)** • *ISO 27001:2022* • *ISO/IEC 42001:2023* • *SOC 2 Type I* • *SOC 2 Type II* • *configurazione HIPAA-ready (Business Associate Agreement disponibile)* *Le certificazioni e attestazioni si applicano ai prodotti commerciali (Claude for Work*

Ambito di valutazione	OpenAI (ChatGPT Ent./API)	Google (Gemini / Vertex AI)	Microsoft (Azure OpenAI)	Anthropic (Claude Ent./API)
	✓ **Verificato** *ISO 42001: non citata nella pagina ufficiale openai.com/security-and-privacy verificata giugno 2026.* **Fonte:** *openai.com/security-and-privacy* ⚠ **Da verificare** *FedRAMP, HIPAA BAA, CSA STAR: non verificati su fonte ufficiale in questa revisione.* **Verificare su:** *trust.openai.com*	*ISO/IEC 42001:2023 certificato per:* • *Google Cloud Platform* • *Google Workspace* • *Gemini App* • *Vertex AI Platform* • *Vertex AI Search* • *Gemini for Google Cloud* • *Gemini for Google Workspace* • *AI Platform Training and Prediction* • *Document AI* • *Speech-to-Text* • *Text-to-Speech.* **La certificazione riguarda i servizi inclusi nello scope pubblicato da Google; verificare che il servizio concretamente adottato rientri nello scope della certificazione pubblicata da Google.** **Fonte:** *cloud.google.com/security/compliance/iso-42001 (letta giugno 2026)* ✓ **Verificato** *Gemini for Google Workspace rientra nello scope delle certificazioni ISO/IEC 42001, BSI C5 e FedRAMP High.* *Gemini in Chrome non risulta, alla data della presente revisione, ricompreso nello scope delle certificazioni ISO/SOC/FedRAMP indicate per Gemini for Google Workspace.* **Fonte:** *workspace.google.com/security/ai-privacy/ (letta giugno 2026)*	• *ISO/IEC 42001:2023 per Microsoft AI Systems, comprendente Azure AI Foundry Models* **Fonte:** *Microsoft Learn – Azure compliance documentation.* *Microsoft Learn – ISO/IEC 42001 Artificial Intelligence Management System* *Report di audit disponibili tramite Microsoft Service Trust Portal microsoft.com/trust-center*	*e Anthropic API). Non si applicano ai prodotti consumer.* **Fonte** *support.claude.com / privacy.claude.com articolo "What Certifications has Anthropic obtained"* *Report di audit disponibili tramite Anthropic Trust Portal.*
2. Conformità GDPR				
2.1 DPA conforme art. 28 GDPR	**Disponibile** ✓ **Verificato** • *DPA disponibile tramite form su openai.com.* • *OpenAI non accetta DPA del cliente né personalizzazioni.* • *Copre API e piani business (non consumer).* • *Entità contrattuale UE: OpenAI Ireland Ltd.* • *SCC per trasferimenti extra-UE.* **Fonte:** *openai.com/policies/data-processing-addendum (letta giugno 2026)* ⚠ **Da verificare** *Clausole specifiche (audit, carve-out): verificare versione corrente del DPA prima dell'adozione.* **Verificare su:** *openai.com/policies/data-processing-addendum*	**Disponibile** ✓ **Verificato** • *Cloud DPA con SCC.* • *Google opera quale responsabile del trattamento (processor) per i Customer Personal Data disciplinati dal Cloud Data Processing Addendum; il cliente determina il ruolo di titolare o altro ruolo previsto dal GDPR in relazione ai trattamenti effettuati.* • *DPA Workspace auto-incorporato per Core Services.* • *Entità contrattuale UE: Google Ireland Ltd.* **Fonte:** *cloud.google.com/terms/data-processing-addendum (letta giugno 2026)* ⚠ **Da verificare** *Clausole specifiche di audit e data ultima versione: verificare su cloud.google.com/terms.* **Verificare su:** *cloud.google.com/terms/data-processing-addendum*	**Disponibile** ✓ **Verificato** • *SCC;* • *EU-US Data Privacy Framework;* • *Microsoft Ireland Operations Ltd.* *Da gennaio 2026 Anthropic è sub-processor Microsoft per M365 Copilot (coperto da DPA MS).* *Modelli Anthropic esclusi dall'EU Data Boundary.* *Tenant EU/EFTA/UK: Anthropic OFF by default.* *Toggle admin per Word/Excel/PowerPoint dal 3 apr 2026.* *Vecchia modalità 'independent processor' dismessa.* *Gli enti che attivano Claude tramite Microsoft 365 Copilot dovrebbero valutare, secondo il proprio contesto d'uso e*	**Disponibile** ✓ **Verificato** *Il DPA con SCC è incorporato automaticamente nei Commercial Terms.* *Non richiede firma separata. Chi accede a Claude tramite piattaforma terza è soggetto ai termini di quella piattaforma.* **Fonte:** *privacy.claude.com/en/articles/7996862 (letta giugno 2026)* ⚠ **Da verificare** *Clausole specifiche DPA Anthropic: richiedere copia tramite trust.anthropic.com.* **Verificare su:** *trust.anthropic.com*

Ambito di valutazione	OpenAI (ChatGPT Ent./API)	Google (Gemini / Vertex AI)	Microsoft (Azure OpenAI)	Anthropic (Claude Ent./API)
			l'art. 35 GDPR, la necessità di una DPIA. . **Fonte:** *learn.microsoft.com/en-us/microsoft-365/copilot/copilot-anthropic-apps (letta giugno 2026)*	
2.2 Diritti dell'interessato	**Supportato** **Dichiarato dal fornitore** *Privacy Center self-service; DSR; cancellazione propagata.* **Fonte:** *openai.com/policies/privacy-policy* ⚠ **Da verificare** *SLA specifiche DSR: verificare su openai.com.* **Verificare su:** *openai.com*	**Supportato** ✓ **Verificato** *Admin console Workspace; DSR via Google Cloud.* *Il DPA Cloud prevede risposta alle DSR tramite gli strumenti messi a disposizione del cliente.* **Fonte:** *cloud.google.com/terms/data-processing-addendum (letta giugno 2026)* ⚠ **Da verificare** *SLA specifiche DSR: verificare su cloud.google.com.* **Verificare su:** *cloud.google.com*	**Supportato** **Dichiarato dal fornitore** *Microsoft Learn - Microsoft Purview - Microsoft 365 Admin Center* **Fonte:** *microsoft.com/trust-center* ⚠ **Da verificare** *SLA specifiche: verificare su microsoft.com/trust-center.* **Verificare su:** *microsoft.com/trust-center*	**Supportato** **Dichiarato dal fornitore** *Privacy Center Anthropic; DSR gestibili.* *Admin gestisce i dati dell'organizzazione.* **Fonte:** *privacy.claude.com* ⚠ **Da verificare** *SLA specifiche DSR: verificare su privacy.claude.com.* **Verificare su:** *privacy.claude.com*
2.3 Base giuridica del trattamento: la base giuridica dichiarata dal provider nelle proprie privacy policy o nei termini commerciali riguarda i trattamenti effettuati dal provider per proprie finalità o nell'ambito del rapporto contrattuale. L'amministrazione che utilizza il sistema deve individuare autonomamente la base giuridica del proprio trattamento ai sensi dell'art. 6 GDPR e, se del caso, degli artt. 9 e 10 GDPR, distinguendo i trattamenti svolti dal provider quale responsabile ex art. 28 GDPR dagli eventuali trattamenti svolti dal provider come titolare autonomo.	**Parziale** **Dichiarato dal fornitore** *Dichiarata (esecuzione contratto + legittimo interesse) per utenti enterprise e API.* **Fonte:** *openai.com/policies/privacy-policy* ✓ **Verificato** *Garante italiano, provvedimento n. 755 del 2 novembre 2024 (comunicato 20 dicembre 2024): sanzione €15 milioni, campagna informativa 6 mesi.* *Contestati: assenza base giuridica per training, mancata notifica data breach marzo 2023, violazione trasparenza, assenza verifica età.* *Garante ha trasmesso atti al DPC irlandese (autorità capofila) per violazioni continuative.* **Fonte:** *garanteprivacy.it/home/docweb/-/docweb-display/docweb/10085432 (letta giugno 2026)*	**Dichiarata** **Dichiarato dal fornitore** *Esecuzione contratto + legittimo interesse.* *Per alcune funzionalità Google prevede specifici meccanismi di consenso o attivazione da parte del cliente, secondo quanto previsto dalla documentazione del servizio.* **Fonte:** *cloud.google.com/terms/data-processing-addendum* ✓ **Verificato** *CNIL, deliberazione SAN-2025-004 del 1° settembre 2025: Google sanzionata con €325M per visualizzazione di pubblicità tra le email Gmail senza consenso e per deposito di cookie durante creazione account Google senza consenso valido.* *NOTA CRITICA: la sanzione riguarda esclusivamente le pratiche pubblicitarie consumer di Gmail e i cookie, non i servizi cloud o AI enterprise. Non costituisce evidenza di rischio specifico per Google Workspace o Vertex AI Gemini.* **Fonte:** *cnil.fr/en/cookies-and-advertisements-inserted-between-emails-google-fined-325-million-euros-cnil (deliberazione letta giugno 2026)*	**Dichiarata** **Dichiarato dal fornitore** *Le basi giuridiche dichiarate da Microsoft per i trattamenti effettuati quale titolare autonomo sono illustrate nella Microsoft Privacy Statement; il DPA disciplina invece i trattamenti svolti quale responsabile del trattamento.* **Fonte:** *aka.ms/DPA*	**Dichiarata** **Dichiarato dal fornitore** *Commercial Terms e Privacy Policy indicano le basi giuridiche applicabili ai trattamenti effettuati da Anthropic quale titolare; i trattamenti svolti quale responsabile sono disciplinati dai Commercial Terms e dal DPA incorporato.* **Fonte:** *anthropic.com/legal/commercial-terms* ✓ **Verificato** *Consumer (Free, Pro, Max): aggiornamento 28 agosto 2025, scadenza 8 ottobre 2025. Se opt-in: 5 anni. Se non opt-in: 30 giorni. Non si applica ai prodotti commerciali.* **Fonte:** *anthropic.com/news/updates-to-our-consumer-terms (letta giugno 2026)*

Ambito di valutazione	OpenAI (ChatGPT Ent./API)	Google (Gemini / Vertex AI)	Microsoft (Azure OpenAI)	Anthropic (Claude Ent./API)
3. Utilizzo dei dati del cliente per training, debug e miglioramento del servizio				
3.1 Esclusione training su dati cliente (enterprise/API)	**Garantita per API/Enterprise/Business** ✓ **Verificato** *ChatGPT Team rinominato ChatGPT Business il 29 agosto 2025. «By default, we do not use data from ChatGPT Enterprise, ChatGPT Business, ChatGPT Edu [...] or our API platform for training.»* **Fonte:** *help.openai.com/en/articles/12111915 | openai.com/business-data/ (lette giugno 2026)* **Dichiarato dal fornitore** *Consumer Free/Plus: training abilitato di default, opt-out possibile.* **Fonte:** *openai.com/policies/privacy-policy*	**Garantita per Vertex AI / Workspace Enterprise** ✓ **Verificato** *Workspace con Gemini (Business, Enterprise, Education): «Your content is not human reviewed or otherwise used for Generative AI model training outside your domain without permission.»* **Fonte:** *knowledge.workspace.google.com/admin/generative-ai/generative-ai-in-google-workspace-privacy-hub (letta giugno 2026)* ✓ **Verificato** *Vertex AI: i Service Specific Terms prevedono che Google non usi i dati cliente per training salvo permesso.* **Fonte:** *cloud.google.com/terms/service-terms (letta giugno 2026)* **Dichiarato dal fornitore** *Consumer gemini.google.com: i dati possono essere utilizzati per migliorare i servizi secondo quanto previsto dai termini applicabili.. Non idoneo per dati istituzionali.* **Fonte:** *workspace.google.com/security/ai-privacy/*	**Garantita** ✓ **Verificato** *Prompts e completions Azure OpenAI non condivisi con OpenAI né usati per training. Modelli Anthropic via Copilot (sub-processor MS) non usati per training.* **Fonte:** *learn.microsoft.com/en-us/azure/foundry/responsible-ai/openai/data-privacy*	**Garantita per API/commerciale** ✓ **Verificato** *Anthropic non usa dati commerciali per training, salvo opt-in esplicito (Development Partner Program).* **Fonte:** *privacy.claude.com/en/articles/9267385 (letta giugno 2026)* ✓ **Verificato** *Consumer dall'8 ottobre 2025: se opt-in training: 5 anni. Se non opt-in: 30 giorni. Non si applica ai prodotti commerciali.* **Fonte:** *anthropic.com/news/updates-to-our-consumer-terms (letta giugno 2026)*
3.2 Esclusione uso per debug / qualità / monitoring interno	**Parziale / Non esplicita** **Dichiarato dal fornitore** *Abuse monitoring automatico. ZDR disabilita storage.* **Fonte:** *openai.com/security-and-privacy* ⚠ **Da verificare** *Esclusione esplicita debug indiretto su tutti i componenti: non trovata su fonte ufficiale OpenAI.* **Verificare su:** *trust.openai.com*	**Parziale** ✓ **Verificato** *Vertex AI: cache in-memory 24h TTL (non persistence storage), isolata per progetto, rispetta data residency, non viola ZDR.* *Disabilitabile per progetto. Abuse monitoring in-region.* **Fonte:** *docs.cloud.google.com/gemini-enterprise-agent-platform/resources/zero-data-retention (letta giugno 2026)* **Dichiarato dal fornitore** *Workspace: no human review senza consenso.* **Fonte:** *cloud.google.com/terms/data-processing-addendum* ⚠ **Da verificare** *Opt-out abuse logging su Vertex AI: verificare su cloud.google.com/vertex-ai.* **Verificare su:** *cloud.google.com/vertex-ai*	**Condizionato a configurazione** **Dichiarato dal fornitore** *Abuse monitoring automatico in-region (EU) per deployment EU. Human review può essere effettuata da personale autorizzato nei casi previsti dalla documentazione Microsoft e secondo il deployment utilizzato* . **Fonte:** *learn.microsoft.com/en-us/azure/foundry/responsible-ai/openai/data-privacy* ⚠ **Da verificare** *Procedura per disabilitare log storage abuse: verificare su azure.microsoft.com.* **Verificare su:** *azure.microsoft.com*	**Parziale: eccezione rilevante** ✓ **Verificato** *Con ZDR o HIPAA: se contenuto flaggato dai classificatori trust & safety, input/output trattenuti fino a 2 anni, score fino a 7 anni.* *Valido anche con ZDR sia per consumer che per API commerciale.* **Fonte:** *docs.anthropic.com/en/docs/build-with-claude/zero-data-retention (letta giugno 2026)* ✓ **Verificato** *Stessa policy confermata nella retention policy commerciale.* **Fonte:** *privacy.claude.com/en/articles/7996866 (letta giugno 2026)*
4. Residenza dei dati in UE (trattamento, memorizzazione, accesso)				
4.1 Data residency UE (at-rest storage)	**Disponibile (Enterprise, Business, Edu, Healthcare, API)** ✓ **Verificato** *ChatGPT Enterprise, Business, Edu, Healthcare: data residency at-rest disponibile in EU, USA, UK, JP, CA, KR, SG, AU, IN, UAE.* *Enterprise/Edu: anche inference residency in-region.*	**Disponibile: distinzione prodotti rilevante per la PA** ✓ **Verificato** *Vertex AI (Gemini Enterprise Agent Platform): data residency configurabile per regione EU.* *Endpoint regionale che mantiene i dati nella regione selezionata secondo la documentazione Google.* *L'endpoint globale non offre garanzie di residenza. ZDR disponibile.* **Fonte:** *docs.cloud.google.com/vertex-ai/generative-ai/docs/learn/data-residency (letta giugno 2026)*	**Disponibile con EU DataZone** **Dichiarato dal fornitore** *EU Data Zone Standard prevede che input, output e log siano trattati nell'EU Data Boundary secondo la documentazione Microsoft. Global Standard: dati possono uscire dall'UE.* **Fonte:** *learn.microsoft.com/en-us/azure/foundry/responsible-ai/openai/data-privacy* ✓ **Verificato**	**Dipende dal deployment** ✓ **Verificato** *API Anthropic diretta: il parametro inference_geo supporta solo 'us' (inferenza solo su infrastruttura USA) e 'global' (inferenza in qualsiasi area disponibile per performance ottimale).* *Il valore 'eu' non è disponibile. Il workspace geo è attualmente disponibile solo come 'us'.*

Ambito di valutazione	OpenAI (ChatGPT Ent./API)	Google (Gemini / Vertex AI)	Microsoft (Azure OpenAI)	Anthropic (Claude Ent./API)
	Fonte: *openai.com/business-data/ | help.openai.com/en/articles/9903489 (lette giugno 2026)* **✓ Verificato** *API Platform: data residency configurabile per progetto (US o Europa). Non modificabile successivamente.* *Apps con sync supportate in USA/Europa/Giappone.* *Alcune funzionalità limitate in EU: `background=True` non disponibile, extended prompt caching può uscire dalla regione, app esterne usano le proprie policy.* **Fonte:** • *platform.openai.com/docs/guides/your-data* • *help.openai.com/en/articles/9903489 (lette giugno 2026)*	**✓ Verificato** *Google Workspace con Gemini Enterprise: data residency in US o EU. No training senza permesso. Gemini 3.5 Flash disponibile in EU da giugno 2026.* **Fonte:** *workspace.google.com/security/ai-privacy/ | docs.cloud.google.com/gemini/enterprise/docs/release-notes (lette giugno 2026)* **✓ Verificato** *Gemini app consumer (gemini.google.com): non coperta da DPA aziendale. Non idonea per dati istituzionali.* **Fonte:** *knowledge.workspace.google.com/admin/generative-ai/generative-ai-in-google-workspace-privacy-hub (letta giugno 2026)*	*Flex Routing (aggiornato maggio 2026): per tenant EU/EFTA creati dopo il 25 marzo 2026 è abilitato di default.* *Inference LLM può avvenire in USA, Canada o Australia durante i picchi di carico. Dati a riposo restano in EU Data Boundary; dati pseudonimizzati limitati possono uscire per sicurezza operativa.* *Verificare il setting nel Microsoft 365 admin center (Copilot → Settings → Flex routing during peak load periods).* **Fonte:** *learn.microsoft.com/en-us/microsoft-365/copilot/copilot-flex-routing (letta giugno 2026)*	***CONSEGUENZA**: non esiste pinning EU sull'API diretta Anthropic.* ***La versione precedente di questo documento citavano un pinning regionale EU su API diretta basandosi su fonti secondarie: una ricerca più accurata non ha permesso di verificare la disponibilità di quella informazione su fonti ufficiali. Pertanto quella informazione è da ritenersi ERRATA.*** **Fonte:** *platform.claude.com/docs/en/manage-claude/data-residency (letta giugno 2026)* **✓ Verificato** *Per residenza EU dei dati: obbligatorio usare AWS Bedrock EU-region (eu-central-1 Frankfurt, eu-west-1 Ireland, eu-north-1 Stockholm) o Vertex AI EU regions.* *I dati commerciali sono archiviati negli USA per default. Il traffico può essere instradato in Europa, Asia e Australia, ma senza garanzia contrattuale EU-only.* **Fonte:** *privacy.claude.com/en/articles/7996890 (letta giugno 2026)* **✓ Verificato** *Microsoft Foundry (Azure): supporto EU in programma per 2026, ma non ancora disponibile. Attualmente l'inference avviene su infrastruttura Anthropic USA anche via Foundry.* **Fonte:** *learn.microsoft.com/en-us/answers/questions/5867930 (letta giugno 2026)*
4.2 Elaborazione (inference) in-region UE	**Disponibile (Enterprise, Edu, Healthcare; API su endpoint EU)** **✓ Verificato** *ChatGPT Enterprise/Edu/Healthcare: inference residency in Europa (EEA + Svizzera).* *GPU inference in-region; altri processing possono avvenire fuori regione.* **Fonte:** *help.openai.com/en/articles/9903489 (letta giugno 2026)* **✓ Verificato** *API Platform: inference in-region (US o Europa) su endpoint regionali per modelli supportati. `background=True` non disponibile in EU. Extended prompt caching può uscire dalla regione.* **Fonte:** *platform.openai.com/docs/guides/your-data (letta giugno 2026)*	**Disponibile (Vertex AI / Gemini Enterprise)** **✓ Verificato** *Vertex AI: endpoint locali EU disponibili e garantiscono ML processing in-region.* *L'endpoint globale non offre garanzie. Gemini 3.5 Flash disponibile in EU da giugno 2026 (GA in US/EU/global).* *Workspace con Gemini: elaborazione EU configurabile per edizioni enterprise.* *Fonte: workspace.google.com/security/ai-privacy/* **Fonte:** - *docs.cloud.google.com/vertex-ai/generative-ai/docs/learn/data-residency* - *docs.cloud.google.com/gemini/enterprise/docs/release-notes (lette giugno 2026)* - *workspace.google.com/security/ai-privacy/*	**EU DataZone / Regional Standard** **Dichiarato dal fornitore** *Con EU DataZone o Regional Standard EU: inference garantita in-region. Global Standard: inference globale.* **Fonte:** *learn.microsoft.com/en-us/azure/foundry/responsible-ai/openai/data-privacy* **✓ Verificato** *Flex Routing: se abilitato, inference può avvenire fuori EU anche con EU DataZone attivo.* **Fonte:** *learn.microsoft.com/en-us/microsoft-365/copilot/copilot-flex-routing (letta giugno 2026)*	**Solo via CSP di supporto** **✓ Verificato** *Inference EU garantita solo via AWS Bedrock EU-region o Vertex AI EU. API diretta Anthropic: inference_geo 'eu' non disponibile. Solo 'us' e 'global'.* *Microsoft Foundry EU: in sviluppo per 2026, non ancora disponibile.* **Fonte:** *platform.claude.com/docs/en/manage-claude/data-residency (letta giugno 2026)*

Ambito di valutazione	OpenAI (ChatGPT Ent./API)	Google (Gemini / Vertex AI)	Microsoft (Azure OpenAI)	Anthropic (Claude Ent./API)
4.3 Accesso ai dati limitato a personale UE	**Non dichiarato esplicitamente** **Dichiarato dal fornitore** *Sede USA. DPA impone SCC ma non restringe geograficamente l'accesso operativo del personale a UE.* **Fonte:** *openai.com/policies/data-processing-addendum* **⚠ Da verificare** *Dichiarazione esplicita di limitazione accessi a personale UE: non trovata su fonte ufficiale OpenAI.* **Verificare su:** *trust.openai.com*	**Parziale** **✓ Verificato** *Il DPA Cloud prevede controlli per limitare l'accesso ai Customer Data da parte del personale di supporto, inclusa la possibilità di limitare l'accesso a personale del provider in specifiche aree geografiche per clienti con requisiti di data residency.* **Fonte:** *cloud.google.com/terms/data-processing-addendum (letta giugno 2026)* **⚠ Da verificare** *Copertura specifica per Vertex AI e dettaglio operativo degli accessi: verificare su cloud.google.com.* **Verificare su:** *cloud.google.com*	**Parzialmente garantito** **Dichiarato dal fornitore** *La documentazione Microsoft sull'EU Data Boundary prevede misure per limitare l'accesso ai dati da parte del personale di supporto del provider, con specifiche eccezioni e meccanismi organizzativi. La copertura deve essere verificata per il servizio Azure OpenAI effettivamente utilizzato.* **Fonte:** *learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn* **⚠ Da verificare** *Data Guardian e dettagli per Azure OpenAI: verificare su azure.microsoft.com.* **Verificare su:** *azure.microsoft.com*	**Non dichiarato** **⚠ Da verificare** *Dichiarazione di limitazione geografica del personale del provider con accesso operativo: non trovata su fonte ufficiale Anthropic.* **Verificare su:** *trust.anthropic.com*
5. Logging: contenuto, dettaglio e configurabilità				
5.1 Descrizione contenuto log	**Parziale** **Dichiarato dal fornitore** *OpenAI effettua attività automatizzate di abuse monitoring. L'eventuale configurazione Zero Data Retention esclude la conservazione dei contenuti per gli endpoint e le funzionalità compatibili, ma non il trattamento necessario all'erogazione del servizio. La conservazione di dati tecnici e amministrativi deve essere verificata in relazione al prodotto, all'endpoint e alla configurazione adottati.* **Fonte:** *platform.openai.com/docs/guides/your-data* **✓ Verificato** *Per ChatGPT Enterprise ed Edu, la Compliance Platform consente l'accesso a log e metadati del workspace tramite una piattaforma di log di conformità immutabili e una Stateful Compliance API.* *Per la piattaforma API, l'Audit Logs API registra eventi relativi alle attività amministrative e alla configurazione dell'organizzazione, quali gestione delle chiavi API e degli inviti; non costituisce un log generale del contenuto di prompt e risposte.* **Fonte:** *help.openai.com/en/articles/9261474-openai-compliance-*	**Parziale** **✓ Verificato** *Vertex AI supporta configurazioni Zero Data Retention. Alcune funzionalità possono comportare conservazione temporanea: ad esempio, l'attivazione della Session Resumption per Gemini Live API comporta la conservazione in cache di prompt e output fino a 24 ore. Per conseguire ZDR, tali funzionalità devono essere disabilitate o non utilizzate.* *Google può effettuare il logging dei prompt per finalità di rilevazione degli abusi nei casi previsti dai termini applicabili. I clienti soggetti a tale logging possono richiedere un'esenzione secondo la procedura prevista da Google.* **Fonte:** - *docs.cloud.google.com/ vertex-ai/generative-ai/docs/vertex-ai-zero-data-retention* - *docs.cloud.google.com/vertex-ai/generative-ai/docs/learn/abuse-monitoring* **✓ Verificato** Google Workspace mette a disposizione log ed eventi amministrativi relativi all'utilizzo di Gemini tramite gli strumenti di reporting e investigazione di Workspace **Dichiarato dal fornitore** *Workspace: Cloud Audit Logs disponibili per export.* **Fonte:** *workspace.google.com/security/ai-privacy/* **⚠ Da verificare** *Verificare, per l'edizione Workspace adottata, quali eventi Gemini siano disponibili, il relativo contenuto e i periodi di conservazione.* **Verificare su:** *cloud.google.com*	**Documentato e configurabile** **✓ Verificato** *Azure OpenAI espone tramite Azure Monitor metriche e log di piattaforma relativi, tra l'altro, a richieste, utilizzo, token, errori e latenza. I resource logs devono essere abilitati e instradati mediante diagnostic settings.* *Il contenuto di prompt e risposte non è incluso automaticamente nei normali log di piattaforma. L'eventuale logging del contenuto richiede una configurazione separata a livello applicativo o tramite componenti di gateway, con conseguenti implicazioni di protezione dei dati* **Fonte:** learn.microsoft.com/en-us/azure/foundry/openai/monitor-openai-reference | learn.microsoft.com/en-us/azure/architecture/ai-ml/guide/azure-openai-gateway-monitoring **⚠ Condizionato** *I clienti che soddisfano i requisiti di Limited Access possono chiedere l'accesso al programma Modified Abuse Monitoring. La modifica non è disponibile automaticamente e può essere soggetta a condizioni più restrittive per determinati modelli..* **Verificare su:** *learn.microsoft.com/en-us/azure/foundry/openai/concepts/abuse-monitoring*	**Documentato con eccezioni rilevanti** **✓ Verificato** *Per i prodotti e le funzionalità coperti da un accordo Zero Data Retention, Anthropic non conserva ordinariamente input e output dopo l'erogazione della risposta, fatte salve le eccezioni previste dalle condizioni applicabili.* *Se una chat o una sessione è segnalata dai sistemi automatizzati di trust and safety come possibile violazione della Usage Policy, Anthropic può conservare input e output fino a 2 anni e i relativi punteggi di classificazione fino a 7 anni..* **Fonte:** *privacy.claude.com/en/articles/8956058 | privacy.claude.com/en/articles/799686 (letta giugno 2026)* **⚠ Da verificare** *Verificare che il modello, il prodotto e le funzionalità concretamente utilizzati rientrino nell'accordo ZDR e non siano soggetti a specifiche regole di conservazione..*

Ambito di valutazione	OpenAI (ChatGPT Ent./API)	Google (Gemini / Vertex AI)	Microsoft (Azure OpenAI)	Anthropic (Claude Ent./API)
	platform-for-enterprise-customers *help.openai.com/en/articles/9687866-admin-and-audit-logs-api-for-the-api-platform* **⚠ Da verificare** *Verificare nella documentazione riservata della Compliance Platform il dettaglio dei contenuti e dei metadati effettivamente disponibili per il piano adottato.* **Verificare su:** *trust.openai.com*			
5.2 Log e audit esportabili	**Disponibile (Enterprise); Limitato per Business, e API)** **✓ Verificato** *ChatGPT Enterprise ed Edu: Compliance Platform per l'acquisizione di log e metadati del workspace e per l'integrazione con strumenti eDiscovery, DLP, SIEM o data lake.* *API Platform: Audit Logs API per l'esportazione degli eventi relativi alle azioni amministrative e alle modifiche della configurazione dell'organizzazione..* **Fonte:** *help.openai.com/en/articles/9261474-openai-compliance-platform-for-enterprise-customers | help.openai.com/en/articles/9687866-admin-and-audit-logs-api-for-the-api-platform* **⚠ Da verificare** *Verificare la disponibilità di funzionalità equivalenti per ChatGPT Business e l'eventuale esportazione dei contenuti delle richieste e delle risposte API, che non risulta coperta dall'Audit Logs API.* **Verificare su:** *platform.openai.com*	**Disponibile con configurazione differenziata per tipologia di log** **✓ Verificato** *Vertex AI genera Cloud Audit Logs. I log Admin Activity e System Event sono sempre abilitati; i Data Access logs devono generalmente essere abilitati espressamente. I log possono essere consultati e instradati mediante Cloud Logging e Log Router verso destinazioni supportate, inclusi BigQuery e sistemi esterni.* *Google Workspace con Gemini mette a disposizione funzionalità di logging ed esportazione dell'attività Gemini tramite gli strumenti amministrativi e di sicurezza di Workspace.* **Fonte:** *docs.cloud.google.com/vertex-ai/docs/general/audit-logging | docs.cloud.google.com/vertex-ai/generative-ai/docs/enable-audit-logs | workspace.google.com/security/ai-privacy/* **⚠ Da verificare** *erificare le funzionalità effettivamente disponibili nell'edizione Workspace adottata e la configurazione dei Data Access logs per Vertex AI..* **Verificare su:** *cloud.google.com/vertex-ai*	**Disponibile** **✓ Verificato** *Azure OpenAI supporta metriche e resource logs tramite Azure Monitor. Mediante diagnostic settings, i dati possono essere instradati verso Log Analytics, account di archiviazione ed Event Hubs e successivamente integrati con sistemi SIEM..* **Fonte:** *learn.microsoft.com/en-us/azure/foundry/openai/monitor-openai-reference | learn.microsoft.com/en-us/azure/azure-monitor/essentials/diagnostic-settings* **⚠ Da verificare** *Disponibilità specifica per Verificare le categorie di log disponibili per la risorsa e il deployment concretamente utilizzati e la configurazione necessaria per l'integrazione con il SIEM adottato.* **Verificare su:** *azure.microsoft.com*	**Disponibile per Claude Enterprise e Claude Platform, con ambito differenziato** **✓ Verificato** Claude Enterprise dispone di audit log esportabili. Organization Owner e Primary Owner possono esportare i log dell'organizzazione relativi agli ultimi 180 giorni. La Claude Compliance API è disponibile per Claude Enterprise e per i clienti Claude Platform: - per Claude Enterprise consente l'accesso a contenuti delle conversazioni, file caricati, progetti ed eventi del feed di attività; - per Claude Platform consente l'accesso a eventi amministrativi, di sistema e relativi alle risorse; il contenuto delle conversazioni, inclusi prompt e risposte del modello, non è disponibile tramite Compliance API. **Fonte:** *support.claude.com/en/articles/9970975-access-audit-logs | support.claude.com/en/articles/13015708-access-the-compliance-api | support.claude.com/en/articles/15167101-get-started-with-claude-compliance-api-integrations* **⚠ Da verificare** *Verificare l'abilitazione contrattuale della Compliance API, i limiti di retention e l'ambito dei dati disponibili per il piano concretamente adottato..*
6. Politiche di retention di prompt, dati e log				
6.1 Retention log e prompt (default)	**Dichiarata e configurabile**	**Dichiarata** **✓ Verificato**	**Dichiarata e configurabile** **Dichiarato dal fornitore**	**Dichiarata** **Dichiarato dal fornitore**

Ambito di valutazione	OpenAI (ChatGPT Ent./API)	Google (Gemini / Vertex AI)	Microsoft (Azure OpenAI)	Anthropic (Claude Ent./API)
	Dichiarato dal fornitore *ChatGPT Enterprise, Business, Edu e Healthcare: la retention di conversazioni e file è configurabile secondo le impostazioni del workspace.* *API Platform: i log di abuse monitoring possono contenere prompt, completions e metadati derivati e sono conservati, per impostazione predefinita, fino a 30 giorni. I clienti idonei possono richiedere Zero Data Retention (ZDR) o Modified Abuse Monitoring. Alcune funzionalità possono conservare application state secondo quanto previsto dalla documentazione del servizio..* **Fonte:** *help.openai.com/en/articles/8983778 | platform.openai.com/docs/guides/your-data* **⚠ Da verificare** *Verificare la retention effettivamente configurata nel workspace e la compatibilità dell'endpoint API con ZDR o Modified Abuse Monitoring.* **Verificare su:** *help.openai.com*	*Vertex AI supporta configurazioni Zero Data Retention. La cache in-memory (TTL 24 ore), isolata per progetto e non persistente su storage ("non at-rest"), è prevista dalla documentazione ufficiale e può essere disabilitata. Alcune funzionalità (es. Session Resumption, request-response logging, grounding) possono comportare retention specifiche secondo la configurazione adottata..* **Fonte:** *docs.cloud.google.com/gemini-enterprise-agent-platform/resources/zero-data-retention (letta giugno 2026)* **⚠ Da verificare** *Default retention Cloud Logging: verificare su cloud.google.com.* **Verificare su:** *cloud.google.com*	*Nell'inferenza stateless ordinaria, Azure OpenAI non conserva prompt e completion dopo l'elaborazione. Alcune funzionalità stateful (ad esempio Responses API, Assistants, Files e Vector Store) conservano dati per consentire l'erogazione del servizio. Il trattamento per abuse monitoring segue le modalità descritte nella documentazione Microsoft; i clienti ammessi possono richiedere il programma Modified Abuse Monitoring..* **Fonte:** *learn.microsoft.com/en-us/azure/foundry/responsible-ai/openai/data-privacy* **⚠ Da verificare** *Verificare la retention delle funzionalità stateful utilizzate.* **Verificare su:** *azure.microsoft.com*	*Anthropic API: input e output sono eliminati automaticamente entro 30 giorni, salvo accordi specifici, esigenze di sicurezza o obblighi di legge. Claude for Work ed Enterprise conservano le conversazioni per l'erogazione del servizio fino alla loro eliminazione da parte del cliente; dopo la cancellazione sono rimosse dai sistemi backend entro 30 giorni. Le chat Incognito sono eliminate entro 30 giorni salvo flagging.* **Fonte:** *privacy.claude.com/en/articles/7996866 (letta giugno 2026)* **✓ Verificato** *ZDR disponibile per clienti qualificati API e Claude Code for Enterprise. Non incluso nel piano Enterprise standard; abilitato su base individuale.* **Fonte:** *privacy.claude.com/en/articles/8956058 (letta giugno 2026)*
6.2 Separazione tra retention operativa e training	**Separazione documentata con limitazioni** **Dichiarato dal fornitore** *I dati trasmessi tramite API non sono utilizzati per l'addestramento dei modelli salvo opt-in esplicito del cliente. La retention per abuse monitoring e l'eventuale conservazione dell'application state sono finalità distinte dal training.* **Fonte:** *platform.openai.com/docs/guides/your-data* **⚠ Da verificare** *Esclusione esplicita log per debug/quality evaluation: non trovata su fonte ufficiale OpenAI.* **Verificare su:** *trust.openai.com*	**Separazione documentata** **✓ Verificato** *Per Vertex AI, la cache in-memory è utilizzata esclusivamente per ridurre la latenza del servizio e non costituisce persistenza dei dati. Per Workspace con Gemini, Google dichiara che prompt e risposte non sono utilizzati per l'addestramento dei modelli generativi al di fuori del dominio del cliente senza autorizzazione* . **Fonte:** *docs.cloud.google.com/gemini-enterprise-agent-platform/resources/zero-data-retention | knowledge.workspace.google.com/admin/generative-ai/generative-ai-in-google-workspace-privacy-hub (letta giugno 2026)*	**Separazione documentata** **Dichiarato dal fornitore** *Prompt, completion e dati cliente non sono utilizzati per addestrare o migliorare i modelli Microsoft o di terzi senza autorizzazione del cliente. Il trattamento effettuato per abuse monitoring è distinto dalle attività di training.* **Fonte:** *learn.microsoft.com/en-us/azure/foundry/responsible-ai/openai/data-privacy* **⚠ Da verificare** *Aggiornamento copertura tutti i componenti: verificare su azure.microsoft.com.* **Verificare su:** *azure.microsoft.com*	**Separazione documentata con eccezioni** **Dichiarato dal fornitore** *Anthropic dichiara di non utilizzare i dati dei prodotti commerciali per l'addestramento dei modelli, salvo adesione volontaria ai programmi previsti dalla documentazione commerciale.* **Fonte:** *privacy.claude.com/en/articles/9267385* **✓ Verificato** *La documentazione ufficiale prevede che i contenuti segnalati per possibile violazione della Usage Policy possano essere conservati secondo la retention policy commerciale.* **Fonte:** *privacy.claude.com/en/articles/7996866 (letta giugno 2026)*
7. Cifratura dati in transito e a riposo				
7.1 Cifratura in transito	**TLS 1.2+ e AES-256 verificati** **✓ Verificato**	**TLS e AES-256 dichiarati** **Dichiarato dal fornitore**	**TLS 1.2+ e AES-256 dichiarati** **Dichiarato dal fornitore**	**TLS e AES-256 dichiarati** **Dichiarato dal fornitore**

Ambito di valutazione	OpenAI (ChatGPT Ent./API)	Google (Gemini / Vertex AI)	Microsoft (Azure OpenAI)	Anthropic (Claude Ent./API)
	AES-256 per dati a riposo. TLS 1.2+ in transito. **Fonte:** *openai.com/business-data/ (letta giugno 2026)*	*TLS per le comunicazioni in transito. AES-256 per dati a riposo.* **Fonte:** *cloud.google.com/security/encryption* **⚠ Da verificare** *Versione TLS specifica: verificare su cloud.google.com/security.* **Verificare su:** *cloud.google.com/security*	*TLS per tutte le comunicazioni cliente-Azure. AES-256 per dati a riposo.* **Fonte:** *azure.microsoft.com/en-us/support/legal/* **⚠ Da verificare** *Standard aggiornati per Azure OpenAI: verificare su azure.microsoft.com.* **Verificare su:** *azure.microsoft.com*	*Comunicazioni cifrate in transito. AES-256 per dati a riposo.* **Fonte:** *privacy.claude.com* **⚠ Da verificare** *Versione TLS e copertura completa: verificare su trust.anthropic.com.* **Verificare su:** *trust.anthropic.com*
7.2 Cifratura a riposo, CMK/BYOK	**EKM disponibile (Enterprise e Edu)** **✓ Verificato** *EKM (BYOK): AWS KMS, GCP Cloud KMS, Azure Key Vault. Richiede accordo con account representative OpenAI. Disponibile per Enterprise e Edu e per API Platform.* **Fonte:** *help.openai.com/en/articles/20000943 (letta giugno 2026)* **✓ Verificato** *Con EKM abilitato: le apps con funzionalità sync diventano non disponibili ('connector' rinominati 'apps' il 17 dic 2025). EKM su ChatGPT Enterprise: disabilita anche workspace agents al lancio.* **Fonte:** *help.openai.com/en/articles/10847137 | help.openai.com/en/articles/10128477 (lette giugno 2026)* **✓ Verificato** *Rotazione chiavi: DEK rotation ogni 24h (path cifratura), ogni ora (path decifratura). Revoca: disabilita accesso a conversazioni precedenti su Enterprise e batch/fine-tuned models su API.* **Fonte:** *help.openai.com/en/articles/20000957 (letta giugno 2026)*	**CMEK disponibile** **Dichiarato dal fornitore** *CMEK su Vertex AI e Google Cloud. Cloud KMS o HSM esterno (BYOK).* **Fonte:** *cloud.google.com/kms* **⚠ Da verificare** *Disponibilità CMEK per Workspace Gemini: verificare su cloud.google.com.* **Verificare su:** *cloud.google.com*	**CMK disponibile** **Dichiarato dal fornitore** *Azure Key Vault + Customer-Managed Keys per Azure OpenAI (per i servizi che supportano CMK).* **Fonte:** *azure.microsoft.com/en-us/products/key-vault* **⚠ Da verificare** *HSM dedicato per Azure OpenAI: verificare su azure.microsoft.com.* **Verificare su:** *azure.microsoft.com*	**Solo via CSP** **Dichiarato dal fornitore** *API diretta: nessuna gestione chiavi client-side documentata. Via AWS Bedrock: AWS KMS + BYOK. Via Azure: Azure Key Vault.* **Fonte:** *privacy.claude.com* **⚠ Da verificare** *BYOK su API diretta Anthropic: verificare su trust.anthropic.com.* **Verificare su:** *trust.anthropic.com*
8. Rotazione, revoca e isolamento chiavi per tenant				
8.1 Rotazione, revoca e isolamento per tenant	**Documentata** **✓ Verificato** *Rotazione DEK: ogni 24h (cifratura), ogni ora (decifratura). Revoca immediata. Il cliente gestisce la master key (KEK) nel proprio KMS; OpenAI non la vede né la conserva.* **Fonte:** *help.openai.com/en/articles/20000957 | help.openai.com/en/articles/20000945 (lette giugno 2026)*	**Documentata** **Dichiarato dal fornitore** *Cloud KMS: rotazione automatica e manuale, revoca immediata. Isolamento per progetto/tenant garantito.* **Fonte:** *cloud.google.com/kms*	**Documentata** **Dichiarato dal fornitore** *Azure Key Vault: rotazione automatica, revoca, audit. Isolamento per tenant Microsoft Entra ID.* **Fonte:** *azure.microsoft.com/en-us/products/key-vault*	**Solo via CSP** **Dichiarato dal fornitore** *Funzionalità KMS delegate al CSP (AWS/Azure). Nessuna feature KMS nativa Anthropic.* **Fonte:** *privacy.claude.com*
9. Controllo accessi privilegiati del fornitore				

QUADRO SINOTTICO: COMPLIANCE NIS2/GDPR/AI ACT: PROVIDER AI

Ambito di valutazione	OpenAI (ChatGPT Ent./API)	Google (Gemini / Vertex AI)	Microsoft (Azure OpenAI)	Anthropic (Claude Ent./API)
9.1 Dichiarazione e limitazione accessi interni	**Parziale** **Dichiarato dal fornitore** *Politica zero-trust e defense-in-depth. Security team on-call 24/7/365.* **Fonte:** *openai.com/business-data/ | openai.com/security-and-privacy* **⚠ Da verificare** *Meccanismi JIT e audit trail per accessi interni: non trovati su fonte ufficiale OpenAI.* **Verificare su:** *trust.openai.com*	**Access Transparency disponibile per Vertex AI** **✓ Verificato** *Access Transparency è disponibile per Vertex AI (incluso Vertex AI Search, Vertex AI Agent Engine). Fornisce log in tempo reale delle azioni del personale Google quando accede ai contenuti del cliente. Richiede che il progetto risieda in un'organizzazione Google Cloud. I log sono integrabili con Cloud Logging e SIEM esistenti.* **Fonte:** *docs.cloud.google.com/vertex-ai/docs/general/access-transparency (letta giugno 2026)* **✓ Verificato** *Access Approval (approvazione esplicita del cliente per accessi Google) supporta Vertex AI Search in GA e Vertex AI Agent Engine. Richiede piano di supporto Google Cloud Standard, Enhanced o Premium per Access Transparency.* **Fonte:** *cloud.google.com/security/products/access-transparency | docs.cloud.google.com/assured-workloads/access-approval/docs/release-notes (lette giugno 2026)*	**Customer Lockbox. ATTENZIONE: non applicabile ad Azure OpenAI per default** **✓ Verificato** *Azure OpenAI Service non rientra nell'ambito di applicazione del Customer Lockbox salvo diversa indicazione della documentazione del servizio specifico.* **Fonte:** *learn.microsoft.com/en-us/power-platform/admin/about-lockbox (letta giugno 2026)* **✓ Verificato** *Customer Lockbox per Microsoft Azure è disponibile per i servizi Azure elencati nella documentazione ufficiale. Richiede piano di supporto Azure con livello minimo Developer. Utilizza JIT (Just-In-Time) access per le richieste di supporto.* **Fonte:** *learn.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview (letta giugno 2026)* **⚠ Da verificare** *Verificare se Azure OpenAI Service specificamente rientra tra i servizi coperti dal Customer Lockbox per Azure consultando la lista aggiornata dei servizi supportati.* **Verificare su:** *learn.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview*	**Non dettagliato** **⚠ Da verificare** *Dichiarazione pubblica su accessi interni ai dati clienti e meccanismi equivalenti a Lockbox o Access Transparency: non trovata su trust.anthropic.com in questa revisione.* **Verificare su:** *trust.anthropic.com*
9.2 Accessi just-in-time e auditabili	**Non dichiarato esplicitamente** **Dichiarato dal fornitore** *Zero trust come principio.* **Fonte:** *openai.com/security-and-privacy* **⚠ Da verificare** *JIT access come feature disponibile al cliente: non trovato su fonte ufficiale OpenAI.* **Verificare su:** *trust.openai.com*	**Documentato** **✓ Verificato** *Access Approval è disponibile per Vertex AI (GA). Consente al cliente di approvare o rifiutare le richieste di accesso del personale Google. I log di Access Transparency coprono Vertex AI.* **Fonte:** *docs.cloud.google.com/assured-workloads/access-approval/docs/release-notes | docs.cloud.google.com/vertex-ai/docs/general/access-transparency (lette giugno 2026)*	**Documentato con limitazioni** **✓ Verificato** *Azure Customer Lockbox usa JIT (Just-In-Time) access per le richieste di supporto. Audit trail completo disponibile nel portale Azure.* **Fonte:** *learn.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview (letta giugno 2026)* **✓ Verificato** *ATTENZIONE: Customer Lockbox NON si applica di default ad Azure OpenAI Service. Verificare se il servizio rientra tra quelli coperti nella lista aggiornata Microsoft.* **Fonte:** *learn.microsoft.com/en-us/power-platform/admin/about-lockbox (letta giugno 2026)*	**Non dichiarato** **⚠ Da verificare** *JIT access e audit trail per accessi interni: non trovati su fonte ufficiale Anthropic.* **Verificare su:** *trust.anthropic.com*
10. Gestione incidenti e notifica violazioni				
10.1 Procedure incident	**Documentate**	**Documentate** **Dichiarato dal fornitore**	**Documentate** **Dichiarato dal fornitore**	**Documentate (nel DPA)** **Dichiarato dal fornitore**

Ambito di valutazione	OpenAI (ChatGPT Ent./API)	Google (Gemini / Vertex AI)	Microsoft (Azure OpenAI)	Anthropic (Claude Ent./API)
response dichiarate	**Dichiarato dal fornitore** *Security response team on-call 24/7/365. DPA include obblighi incident response.* **Fonte:** *openai.com/business-data/* **⚠ Da verificare** *tandard specifici (ISO 27035) e penetration test..* **Verificare su:** *trust.openai.com*	*Google Cloud: procedure IR documentate. DPA include IR. FedRAMP richiede piani IR certificati.* **Fonte:** *cloud.google.com/terms/data-processing-addendum*	*Microsoft Security Response Center (MSRC). DPA con IR.* **Fonte:** *microsoft.com/en-us/msrc* **⚠ Da verificare** *ISO 27035 per IR su Azure OpenAI: verificare su azure.microsoft.com.* **Verificare su:** *azure.microsoft.com*	*Procedure IR nel DPA.* **Fonte:** *privacy.claude.com* **⚠ Da verificare** *Contenuto specifico procedure IR: richiedere tramite trust.anthropic.com.* **Verificare su:** *trust.anthropic.com*
10.2 Notifica violazione dati: obblighi del responsabile verso il titolare e obblighi del titolare verso l'autorità	**Obblighi di notifica disciplinati nel DPA** **Dichiarato dal fornitore** *Il DPA disciplina la notifica al cliente in caso di Personal Data Breach. (GDPR art. 33).* **Fonte:** *openai.com/policies/data-processing-addendum* In caso di violazione dei dati personali, ove il provider operi come responsabile del trattamento, il parametro giuridico da verificare nel DPA è la notifica al titolare senza ingiustificato ritardo dopo la conoscenza della violazione. Il termine di 72 ore riguarda la notifica del titolare all'autorità di controllo, ove dovuta, ai sensi dell'art. 33, par. 1, GDPR. Verificare nel DPA corrente il termine contrattuale assunto dal provider verso il cliente/titolare e il contenuto minimo della notifica.	**Obblighi di notifica disciplinati nel DPA** **✓ Verificato** *Il Cloud DPA prevede notifica al cliente «senza ingiustificato ritardo» dopo che Google viene a conoscenza di un data breach che coinvolge Customer Personal Data.* **Fonte:** *cloud.google.com/terms/data-processing-addendum (letta giugno 2026)* In caso di violazione dei dati personali, ove il provider operi come responsabile del trattamento, il parametro giuridico da verificare nel DPA è la notifica al titolare senza ingiustificato ritardo dopo la conoscenza della violazione. Il termine di 72 ore riguarda la notifica del titolare all'autorità di controllo, ove dovuta, ai sensi dell'art. 33, par. 1, GDPR. Verificare nel DPA corrente il termine contrattuale assunto dal provider verso il cliente/titolare e il contenuto minimo della notifica.	**Obblighi di notifica disciplinati nel DPA** **Dichiarato dal fornitore** *Microsoft DPA: Il DPA disciplina la notifica al cliente in caso di Personal Data Breach. MSRC referente per breach.* **Fonte:** *aka.ms/DPA* In caso di violazione dei dati personali, ove il provider operi come responsabile del trattamento, il parametro giuridico da verificare nel DPA è la notifica al titolare senza ingiustificato ritardo dopo la conoscenza della violazione. Il termine di 72 ore riguarda la notifica del titolare all'autorità di controllo, ove dovuta, ai sensi dell'art. 33, par. 1, GDPR. Verificare nel DPA corrente il termine contrattuale assunto dal provider verso il cliente/titolare e il contenuto minimo della notifica.	**Obblighi di notifica disciplinati nel DPA** **Dichiarato dal fornitore** *DPA Anthropic: Il DPA disciplina la notifica al cliente in caso di Personal Data Breach..* **Fonte:** *privacy.claude.com* In caso di violazione dei dati personali, ove il provider operi come responsabile del trattamento, il parametro giuridico da verificare nel DPA è la notifica al titolare senza ingiustificato ritardo dopo la conoscenza della violazione. Il termine di 72 ore riguarda la notifica del titolare all'autorità di controllo, ove dovuta, ai sensi dell'art. 33, par. 1, GDPR. Verificare nel DPA corrente il termine contrattuale assunto dal provider verso il cliente/titolare e il contenuto minimo della notifica.
11. Minimizzazione dei dati (log e monitoring)				
11.1 Limitazione registrazione contenuto prompt nei log	**Condizionato a ZDR** **Dichiarato dal fornitore** *ZDR elimina la persistenza. Senza ZDR: input/output registrati per abuse monitoring.* **Fonte:** *openai.com/security-and-privacy* **⚠ Da verificare** *Minimizzazione by-design senza ZDR: non documentata esplicitamente su fonte ufficiale OpenAI.* **Verificare su:** *trust.openai.com*	**Richiede configurazione attiva** **✓ Verificato** *Vertex AI ZDR disponibile. Cache in-memory 24h TTL non viola ZDR ma va disabilitata per azzerare ogni caching. Non attiva by-default.* **Fonte:** *docs.cloud.google.com/gemini-enterprise-agent-platform/resources/zero-data-retention (letta giugno 2026)* **⚠ Da verificare** *Configurazione completa per minimizzazione su Workspace Gemini: verificare su cloud.google.com.* **Verificare su:** *cloud.google.com*	**Dipende dalla modalità deployment** **Dichiarato dal fornitore** *Default: prompts non conservati dopo risposta (salvo abuse). Per i deployment EU DataZone/EU Data Boundary il trattamento dell'abuse monitoring segue le regole previste dalla documentazione Microsoft.* **Fonte:** *learn.microsoft.com/en-us/azure/foundry/responsible-ai/openai/data-privacy* **✓ Verificato** *Con Flex Routing abilitato: elaborazione può uscire da EU.*	**API con ZDR: più vicino a minimizzazione** **✓ Verificato** *Con ZDR: nessuna persistenza dopo la risposta, salvo contenuti flaggati (2 anni) e score (7 anni).* **Fonte:** *docs.anthropic.com/en/docs/build-with-claude/zero-data-retention (letta giugno 2026)* **✓ Verificato** *Senza ZDR: dati conservati per il servizio, eliminabili dall'utente/admin.* **Fonte:** *privacy.claude.com/en/articles/7996866 (letta giugno 2026)*

Ambito di valutazione	OpenAI (ChatGPT Ent./API)	Google (Gemini / Vertex AI)	Microsoft (Azure OpenAI)	Anthropic (Claude Ent./API)
			Fonte: *learn.microsoft.com/en-us/microsoft-365/copilot/copilot-flex-routing (letta giugno 2026)*	
12. Gestione sub-fornitori e supply chain				
12.1 Elenco sub-processor dichiarato e aggiornato	**Disponibile** **Dichiarato dal fornitore** *Lista sub-processor pubblicata e aggiornata.* **Fonte:** *openai.com/policies/privacy-policy* **⚠ Da verificare** *Finestra notifica preventiva per modifiche: verificare su openai.com.* **Verificare su:** *openai.com*	**Disponibile** **✓ Verificato** *Google Cloud sub-processor list pubblica, aggiornata. DPA Cloud prevede notifica preventiva delle modifiche ai sub-processor e diritto di obiezione del cliente.* **Fonte:** *cloud.google.com/terms/data-processing-addendum | cloud.google.com/terms/subprocessors (lette giugno 2026)*	**Disponibile** **Dichiarato dal fornitore** *Microsoft Trust Center: lista sub-processor aggiornata per Azure.* **Fonte:** *microsoft.com/trust-center* **✓ Verificato** *Da gennaio 2026 Anthropic inclusa come sub-processor Microsoft per M365 Copilot.* **Fonte:** *learn.microsoft.com/en-us/microsoft-365/copilot/copilot-anthropic-apps (letta giugno 2026)*	**Disponibile (nel DPA)** **✓ Verificato** *DPA incorporato nei Commercial Terms include lista sub-processor. Principale sub-processor infrastrutturale: AWS. Per default il traffico può essere instradato in USA, Europa, Asia e Australia. I dati commerciali sono archiviati negli USA.* **Fonte:** *privacy.claude.com/en/articles/7996862 | privacy.claude.com/en/articles/7996890 (lette giugno 2026)* **⚠ Da verificare** *Lista completa sub-processor con localizzazione: richiedere tramite trust.anthropic.com/subprocessors.* **Verificare su:** *trust.anthropic.com/subprocessors*
12.2 Localizzazione e trattamenti sub-processor	**Parziale** **Dichiarato dal fornitore** *Sub-processor prevalentemente USA. EU data residency limita ma non elimina coinvolgimento sub-processor extra-UE (SCC a copertura).* **Fonte:** *openai.com/policies/privacy-policy* **⚠ Da verificare** *Lista con localizzazione per ciascun sub-processor: verificare su openai.com.* **Verificare su:** *openai.com*	**Dettagliata** **✓ Verificato** *Google Cloud sub-processor list indica localizzazione per ciascuno. I Service Specific Terms prevedono configurazione data location per i servizi in scope. Opzione EU-only disponibile.* **Fonte:** *cloud.google.com/terms/subprocessors | cloud.google.com/terms/service-terms (lette giugno 2026)*	**Dettagliata** **Dichiarato dal fornitore** *Microsoft pubblica localizzazione sub-processor. EU Data Boundary limita il trattamento dei dati personali al perimetro UE/SEE per i servizi coperti, secondo la documentazione Microsoft.* **Fonte:** *microsoft.com/trust-center* **✓ Verificato** *Anthropic (sub-processor da gen. 2026) processa fuori EU Data Boundary.* **Fonte:** *learn.microsoft.com/en-us/microsoft-365/copilot/copilot-anthropic-apps (letta giugno 2026)*	**Meno dettagliata** **Dichiarato dal fornitore** *Lista disponibile nel DPA. AWS (US) principale sub-processor infrastrutturale.* **Fonte:** *privacy.claude.com* **⚠ Da verificare** *Lista aggiornata con localizzazione: richiedere tramite trust.anthropic.com/subprocessors.* **Verificare su:** *trust.anthropic.com/subprocessors*
13. Isolamento tra tenant				
13.1 Isolamento logico/fisico tra clienti diversi	**Dichiarato (logico)** **Dichiarato dal fornitore** *Architettura multi-tenant con isolamento logico dichiarato.* **Fonte:** *openai.com/policies/data-processing-addendum* **⚠ Da verificare** *Certificazione specifica isolamento tenant: verificare su trust.openai.com.* **Verificare su:** *trust.openai.com*	**Dichiarato e certificato** **Dichiarato dal fornitore** *Google Cloud: isolamento per progetto/organizzazione. VPC Service Controls. Certificato da audit SOC 2/ISO.* **Fonte:** *cloud.google.com/security*	**Dichiarato e certificato** **Dichiarato dal fornitore** *Azure: isolamento per tenant Microsoft Entra ID nativo. VNet, NSG, Private Endpoints. Certificato SOC 2/ISO 27001.* **Fonte:** *azure.microsoft.com/en-us/overview/security*	**Dichiarato (logico)** **Dichiarato dal fornitore** *Isolamento logico tra tenant dichiarato. Copertura fisica dipende dal CSP.* **Fonte:** *privacy.claude.com* **⚠ Da verificare** *Certificazione specifica: verificare su trust.anthropic.com.* **Verificare su:** *trust.anthropic.com*

14. Reg. UE 2024/1689 : AI Act (obblighi GPAI e ruolo della PA come deployer)

Calendario applicazione AI Act, sulla base del Reg. UE 2024/1689 vigente:

• 2 febbraio 2025: applicazione dei Capi I e II, incluse le disposizioni su alfabetizzazione in materia di IA e pratiche vietate.
• 2 agosto 2025: applicazione del Capo V sui modelli di IA per finalità generali, del Capo VII, del Capo XII e dell'art. 78, con l'eccezione dell'art. 101.
• 2 agosto 2026: applicazione generale del Regolamento; dalla stessa data si applicano i poteri sanzionatori della Commissione relativi agli obblighi dei provider di modelli GPAI.
• 2 agosto 2027: applicazione dell'art. 6, par. 1, e dei corrispondenti obblighi; entro la stessa data devono conformarsi agli obblighi GPAI anche i provider dei modelli immessi sul mercato prima del 2 agosto 2025.

Eventuali modifiche derivanti da iniziative Omnibus devono essere indicate separatamente e considerate vigenti solo dopo l'adozione definitiva e la pubblicazione dell'atto modificativo nella Gazzetta ufficiale dell'Unione europea.

Ruolo della PA come DEPLOYER: *gli atenei operano normalmente come deployer quando utilizzano sistemi di IA sotto la propria autorità. La qualificazione deve tuttavia essere verificata in concreto: l'ateneo può assumere anche il ruolo di provider nei casi in cui sviluppi o faccia sviluppare un sistema di IA o un modello di IA per finalità generali e lo immetta sul mercato o lo metta in servizio con il proprio nome o marchio, oppure quando ricorrano le condizioni previste dall'art. 25 dell'AI Act.*

14.1 Classificazione come GPAI model (obblighi art. 53 AI Act : trasparenza, documentazione tecnica, copyright : applicabili dal 2 agosto 2025)	**GPAI model : obblighi art. 53 applicabili** ✓ **Verificato** *OpenAI (GPT-4o e modelli successivi) rientra nella definizione GPAI: addestrato con >10^{23} FLOP, genera linguaggio.* *Obblighi art. 53 applicabili dal 2 agosto 2025 per nuovi modelli.* **Fonte:** *digital-strategy.ec.europa.eu/en/policies/guidelines-gpai-providers (letta giugno 2026)* 📋 **Dichiarazioni e documentazione del provider da acquisire** La Commissione considera indicativamente riconducibili alla categoria dei modelli GPAI i modelli addestrati con risorse computazionali superiori a 10^{23} FLOP e capaci di generare linguaggio, immagini o video. La qualificazione del singolo modello utilizzato dall'amministrazione deve essere verificata sulla documentazione ufficiale del provider, sulle informazioni rese disponibili ai soggetti a valle e, ove presenti, sulle indicazioni dell'AI Office. La firma del GPAI Code of Practice non dimostra, da sola, che ogni modello commercializzato dal provider sia un modello GPAI. Se il modello rientra nella categoria GPAI, gli obblighi dell'art. 53 gravano sul provider del modello e comprendono, tra l'altro, documentazione tecnica, informazioni per i provider a valle, una policy sul diritto d'autore e la pubblicazione di una sintesi	**GPAI model : obblighi art. 53 applicabili** ✓ **Verificato** *OpenAI (GPT-4o e modelli successivi) rientra nella definizione GPAI: addestrato con >10^{23} FLOP, genera linguaggio.* *Obblighi art. 53 applicabili dal 2 agosto 2025 per nuovi modelli.* **Fonte:** *digital-strategy.ec.europa.eu/en/policies/guidelines-gpai-providers (letta giugno 2026)* 📋 **Dichiarazioni e documentazione del provider da acquisire** La Commissione considera indicativamente riconducibili alla categoria dei modelli GPAI i modelli addestrati con risorse computazionali superiori a 10^{23} FLOP e capaci di generare linguaggio, immagini o video. La qualificazione del singolo modello utilizzato dall'amministrazione deve essere verificata sulla documentazione ufficiale del provider, sulle informazioni rese disponibili ai soggetti a valle e, ove presenti, sulle indicazioni dell'AI Office. La firma del GPAI Code of Practice non dimostra, da sola, che ogni modello commercializzato dal provider sia un modello GPAI. Se il modello rientra nella categoria GPAI, gli obblighi dell'art. 53 gravano sul provider del modello e comprendono, tra l'altro, documentazione tecnica, informazioni per i provider a valle, una policy sul diritto d'autore e la pubblicazione di una sintesi	**GPAI model : obblighi art. 53 applicabili** ✓ **Verificato** *OpenAI (GPT-4o e modelli successivi) rientra nella definizione GPAI: addestrato con >10^{23} FLOP, genera linguaggio.* *Obblighi art. 53 applicabili dal 2 agosto 2025 per nuovi modelli.* **Fonte:** *digital-strategy.ec.europa.eu/en/policies/guidelines-gpai-providers (letta giugno 2026)* 📋 **Da verificare sul servizio e sul modello adottati** Nel caso di Azure OpenAI, gli obblighi dell'art. 53 relativi al modello GPAI gravano, in linea generale, sul provider del modello sottostante. Microsoft può tuttavia assumere autonomamente obblighi da provider in relazione a propri modelli GPAI o qualora ricorrano le condizioni previste dall'AI Act per i soggetti che modificano o commercializzano modelli a valle. La qualificazione non può essere desunta dalla sola erogazione del modello tramite Azure né dalla firma del GPAI Code of Practice. Deve essere verificata con riferimento al modello specifico, alla catena contrattuale e alle eventuali modifiche apportate. **Fonte:** *Commissione europea, Guidelines for providers of general-purpose AI models.*	**GPAI model : obblighi art. 53 applicabili** ✓ **Verificato** *OpenAI (GPT-4o e modelli successivi) rientra nella definizione GPAI: addestrato con >10^{23} FLOP, genera linguaggio.* *Obblighi art. 53 applicabili dal 2 agosto 2025 per nuovi modelli.* **Fonte:** *digital-strategy.ec.europa.eu/en/policies/guidelines-gpai-providers (letta giugno 2026)* 📋 **Dichiarazioni e documentazione del provider da acquisire** La Commissione considera indicativamente riconducibili alla categoria dei modelli GPAI i modelli addestrati con risorse computazionali superiori a 10^{23} FLOP e capaci di generare linguaggio, immagini o video. La qualificazione del singolo modello utilizzato dall'amministrazione deve essere verificata sulla documentazione ufficiale del provider, sulle informazioni rese disponibili ai soggetti a valle e, ove presenti, sulle indicazioni dell'AI Office. La firma del GPAI Code of Practice non dimostra, da sola, che ogni modello commercializzato dal provider sia un modello GPAI. Se il modello rientra nella categoria GPAI, gli obblighi dell'art. 53 gravano sul provider del modello e comprendono, tra l'altro, documentazione tecnica, informazioni per i provider a valle, una policy sul diritto d'autore e la pubblicazione di una sintesi sufficientemente dettagliata dei

	sufficientemente dettagliata dei contenuti utilizzati per l'addestramento. **Fonte:** *Commissione europea, Guidelines for providers of general-purpose AI models.*	sufficientemente dettagliata dei contenuti utilizzati per l'addestramento. **Fonte:** *Commissione europea, Guidelines for providers of general-purpose AI models.*		contenuti utilizzati per l'addestramento. **Fonte:** *Commissione europea, Guidelines for providers of general-purpose AI models.*
14.2 Modelli GPAI con rischio sistemico, art. 55 AI Act	**Potenzialmente applicabile (da confermare per il singolo modello)** I provider di modelli GPAI con rischio sistemico sono soggetti agli obblighi aggiuntivi dell'art. 55 AI Act. Ai sensi dell'art. 51, un modello GPAI è qualificato come modello con rischio sistemico quando presenta capacità di impatto elevato, valutate sulla base di strumenti e metodologie tecniche adeguati, oppure quando è designato come tale dalla Commissione. Si presume che il modello presenti capacità di impatto elevato quando il quantitativo cumulativo di risorse computazionali utilizzato per il suo addestramento, misurato in FLOP, è superiore a 10^{25}. La classificazione del singolo modello deve risultare da una notifica all'AI Office, da una decisione della Commissione o da documentazione ufficiale verificabile. Non può essere desunta da valutazioni di analisti, dalla notorietà del modello o dalla sola firma del capitolo Safety and Security del GPAI Code of Practice. **Fonte:** *artt. 51, 52 e 55 del Regolamento (UE) 2024/1689; Commissione europea, General-purpose AI obligations under the AI Act.*	**Potenzialmente applicabile (da confermare per il singolo modello)** I provider di modelli GPAI con rischio sistemico sono soggetti agli obblighi aggiuntivi dell'art. 55 AI Act. Ai sensi dell'art. 51, un modello GPAI è qualificato come modello con rischio sistemico quando presenta capacità di impatto elevato, valutate sulla base di strumenti e metodologie tecniche adeguati, oppure quando è designato come tale dalla Commissione. Si presume che il modello presenti capacità di impatto elevato quando il quantitativo cumulativo di risorse computazionali utilizzato per il suo addestramento, misurato in FLOP, è superiore a 10^{25}. La classificazione del singolo modello deve risultare da una notifica all'AI Office, da una decisione della Commissione o da documentazione ufficiale verificabile. Non può essere desunta da valutazioni di analisti, dalla notorietà del modello o dalla sola firma del capitolo Safety and Security del GPAI Code of Practice. **Fonte:** *artt. 51, 52 e 55 del Regolamento (UE) 2024/1689; Commissione europea, General-purpose AI obligations under the AI Act.*	**Dipende dal modello sottostante e dal ruolo assunto da Microsoft** Per i modelli OpenAI erogati tramite Azure, la qualificazione del modello GPAI con rischio sistemico e i relativi obblighi primari devono essere verificati con riferimento al provider del modello sottostante. Microsoft può essere autonomamente soggetta agli artt. 51, 52 e 55 per eventuali propri modelli GPAI qualificati a rischio sistemico. **✓ Verificato** *Microsoft è inclusa nell'elenco dei firmatari del GPAI Code of Practice pubblicato dalla Commissione. La firma del Codice non costituisce, di per sé, prova che uno specifico modello Microsoft sia stato qualificato come GPAI con rischio sistemico.* **Fonte:** *Commissione europea, The General-Purpose AI Code of Practice)*	**Potenzialmente applicabile (da confermare per il singolo modello)** I provider di modelli GPAI con rischio sistemico sono soggetti agli obblighi aggiuntivi dell'art. 55 AI Act. Ai sensi dell'art. 51, un modello GPAI è qualificato come modello con rischio sistemico quando presenta capacità di impatto elevato, valutate sulla base di strumenti e metodologie tecniche adeguati, oppure quando è designato come tale dalla Commissione. Si presume che il modello presenti capacità di impatto elevato quando il quantitativo cumulativo di risorse computazionali utilizzato per il suo addestramento, misurato in FLOP, è superiore a 10^{25}. La classificazione del singolo modello deve risultare da una notifica all'AI Office, da una decisione della Commissione o da documentazione ufficiale verificabile. Non può essere desunta da valutazioni di analisti, dalla notorietà del modello o dalla sola firma del capitolo Safety and Security del GPAI Code of Practice. **Fonte:** *artt. 51, 52 e 55 del Regolamento (UE) 2024/1689; Commissione europea, General-purpose AI obligations under the AI Act.*
14.3 Adesione al GPAI Code of Practice (strumento volontario : lista pubblica Commissione Europea, aggiornata 23 aprile 2026)	**Firmatario del GPAI Code of Practice** **✓ Verificato** *OpenAI è inclusa nell'elenco dei firmatari del GPAI Code of Practice pubblicato dalla Commissione europea e partecipa alla Signatory Taskforce istituita dai firmatari e presieduta dall'AI Office.* *La firma non equivale a certificazione automatica di conformità. Il Codice è uno strumento volontario riconosciuto dalla Commissione e dall'AI Board come mezzo adeguato per dimostrare la conformità, a condizione che il provider rispetti concretamente gli impegni applicabili.* *I poteri di enforcement della Commissione nei confronti dei provider GPAI si applicano dal 2 agosto 2026.* **Fonte:** *Commissione europea, The General-Purpose AI Code of Practice; Guidelines for providers of general-purpose AI models.*	**Firmatario del GPAI Code of Practice** **✓ Verificato** *Google è inclusa nell'elenco dei firmatari del GPAI Code of Practice pubblicato dalla Commissione europea e partecipa alla Signatory Taskforce.* *La firma costituisce adesione volontaria a uno strumento riconosciuto come adeguato per dimostrare la conformità agli obblighi GPAI applicabili, purché siano rispettati concretamente gli impegni sottoscritti.* **Fonte:** *Commissione europea, The General-Purpose AI Code of Practice.*	**Firmatario del GPAI Code of Practice** **✓ Verificato** *Microsoft è inclusa nell'elenco dei firmatari del GPAI Code of Practice pubblicato dalla Commissione europea.* *La firma riguarda gli obblighi applicabili a Microsoft quale provider di eventuali modelli GPAI rientranti nel proprio perimetro. Non consente di qualificare automaticamente Microsoft come provider dei modelli OpenAI erogati tramite Azure né Copilot come modello GPAI.* *Per Azure OpenAI, il ruolo e gli obblighi devono essere distinti tra provider del modello GPAI, provider del sistema a valle e deployer, sulla base della concreta catena di fornitura.* **Fonte:** *Commissione europea, The General-Purpose AI Code of Practice; Regolamento (UE) 2024/1689.*	**Firmatario del GPAI Code of Practice** **✓ Verificato** *Anthropic è inclusa nell'elenco dei firmatari del GPAI Code of Practice pubblicato dalla Commissione europea.* *La firma del Codice costituisce adesione volontaria a uno strumento riconosciuto dalla Commissione e dall'AI Board come adeguato per dimostrare la conformità agli obblighi GPAI applicabili, ferma restando la necessità di rispettare concretamente gli impegni assunti e di fornire all'AI Office la documentazione e le informazioni richieste.* **Fonte:** *Commissione europea, The General-Purpose AI Code of Practice.* La firma del Codice è uno strumento volontario riconosciuto per dimostrare la conformità agli obblighi GPAI, ferma restando la necessità di rispettare

			Per Azure OpenAI: gli obblighi GPAI primari ricadono su OpenAI come provider del modello.	concretamente gli impegni assunti e di fornire documentazione quando richiesta.

NOTE METODOLOGICHE

Rev. giugno 2026 (include AI Act)

Nota metodologica e perimetro normativo del documento

Il presente documento è prodotto dal Gruppo ICT CRUI nell'ambito delle attività di negoziazione, pre-contrattuali e contrattuali con i provider di servizi AI.

È reso disponibile agli enti aderenti ai contratti CRUI come strumento di supporto per le proprie valutazioni in materia di conformità normativa.

Il perimetro normativo copre tre strumenti che si applicano cumulativamente agli stessi provider e agli stessi contratti:

- la Direttiva NIS2 (D.Lgs. 138/2024),
- il Regolamento GDPR (Reg. UE 2016/679),
- il Regolamento AI (Reg. UE 2024/1689).

L'integrazione dell'AI Act in questo documento, anziché in un documento separato, risponde a una scelta di perimetro normativo: trattare in un unico strumento le tre normative che l'ente deve considerare contestualmente nella valutazione di un provider AI, evitando che la frammentazione documentale generi lacune nell'analisi.

Per NIS2 e GDPR il documento valuta i provider nella loro qualità di fornitori della catena di approvvigionamento dell'ente (art. 21 e ss. NIS2; art. 28 GDPR).

Per l'AI Act la distinzione è strutturale: i provider analizzati sono **provider di modelli GPAI** con obblighi propri (artt. 53 e 55 AI Act, applicabili dal 2 agosto 2025), mentre gli enti aderenti assumono il ruolo di **deployer** con obblighi distinti (AI literacy dal 2 febbraio 2025; obblighi per sistemi ad alto rischio dal 2 agosto 2026). La sezione 14 documenta entrambi i livelli. Questa articolazione non sarebbe comunicabile in modo efficace in un documento separato senza duplicare il contesto contrattuale e normativo già sviluppato nelle sezioni precedenti.

Il documento è aggiornato alla revisione di giugno 2026 e tiene conto dell'accordo politico del 7 maggio 2026 sul regolamento modificativo AI Omnibus (le date che ne derivano sono riportate *sub condicione* rispetto all'esito dell'adozione definitiva e della pubblicazione del regolamento modificativo).

Il documento non costituisce parere legale né sostituisce la DPIA o l'analisi del rischio che ciascun ente è tenuto a condurre autonomamente prima dell'adozione di un servizio AI.

1. Sistema di marcatori epistemici

✓ **Verificato**: fonte primaria letta direttamente in questa revisione. Contenuto riportato fedelmente con URL e data di lettura.

Dichiarato dal fornitore: affermazione che proviene da DPA, Product Terms, Privacy Policy o pagine security del fornitore. Non verificata da terzi indipendenti. La PA si fida della dichiarazione contrattuale del fornitore, consapevole che non è una verifica esterna.

Certificazione dichiarata : report richiedibile: il fornitore dichiara di aver ottenuto la certificazione. Il report completo è redatto da ente terzo accreditato ma non è pubblico: va richiesto tramite Trust Center, spesso previo NDA. La PA deve richiedere e leggere il report prima dell'adozione.

⚠ **Da verificare**: fonte non letta direttamente in questa revisione. Non usare in decisioni formali di procurement o DPIA senza aver verificato la fonte indicata.

2. Correzioni critiche rispetto alle versioni precedenti

Anthropic API diretta : data residency EU (4.1 e 4.2): Il parametro inference_geo supporta solo 'us' e 'global'. Il valore 'eu' non è disponibile. Le versioni precedenti citavano un pinning regionale EU basandosi su fonti secondarie: quella informazione pare non corretta. Per residenza EU è obbligatorio usare AWS Bedrock EU-region o Vertex AI EU regions.
Fonte: platform.claude.com/docs/en/manage-claude/data-residency (letta giugno 2026).

Azure OpenAI e Customer Lockbox (9.1 e 9.2): Le funzionalità basate su Azure OpenAI Service sono ESCLUSE dall'applicazione della policy Customer Lockbox, salvo dichiarazione esplicita nella documentazione del prodotto specifico. Le versioni precedenti indicavano il Lockbox come disponibile per Azure OpenAI: era impreciso. Fonte: learn.microsoft.com/en-us/power-platform/admin/about-lockbox (letta giugno 2026).

CNIL multa Google (2.3): La multa CNIL del 1° settembre 2025 (€325M) riguarda le pratiche pubblicitarie consumer di Gmail e i cookie, non i servizi cloud o AI enterprise. Non costituisce evidenza di rischio specifico per Google Workspace o Vertex AI Gemini. La contestualizzazione precedente era fuorviante. Fonte: cnil.fr/en/ (letta giugno 2026).

EDPB su web scraping AI (2.3): Il Work Programme 2026-2027 (adottato 12 febbraio 2026) include adozione di linee guida su AI generativa e data scraping. Le linee guida 03/2026 sul web scraping per AI sono già state adottate e sono in consultazione pubblica fino al 30 ottobre 2026. Non è più solo un'intenzione futura. Fonte: edpb.europa.eu (letta giugno 2026).

Access Transparency per Vertex AI (9.1 e 9.2): Disponibile e documentata su fonte ufficiale Google. Richiede piano di supporto Standard, Enhanced o Premium. Access Approval disponibile per Vertex AI in GA. Versioni precedenti segnalavano questo come da verificare: ora è ✓ verificato. Fonte: docs.cloud.google.com/vertex-ai/docs/general/access-transparency (letta giugno 2026).

3. Fonti primarie lette direttamente in questa revisione

• OpenAI : Business data & privacy: openai.com/business-data/
• OpenAI : Security & Privacy: openai.com/security-and-privacy
• OpenAI : Data residency for ChatGPT (incluso inference residency): help.openai.com/en/articles/9903489
• OpenAI : Data residency API (platform.openai.com): platform.openai.com/docs/guides/your-data
• OpenAI : DPA: openai.com/policies/data-processing-addendum
• OpenAI : ChatGPT Business rename: help.openai.com/en/articles/12111915
• OpenAI : Apps with sync: help.openai.com/en/articles/10847137
• OpenAI : EKM Overview: help.openai.com/en/articles/20000943
• OpenAI : EKM KMS key lifecycle: help.openai.com/en/articles/20000957 | EKM Technical FAQ: help.openai.com/en/articles/20000945
• OpenAI : Enterprise Release Notes: help.openai.com/en/articles/10128477
• Microsoft : Flex routing EU/EFTA: learn.microsoft.com/en-us/microsoft-365/copilot/copilot-flex-routing
• Microsoft : Copilot with Anthropic apps: learn.microsoft.com/en-us/microsoft-365/copilot/copilot-anthropic-apps
• Microsoft : Customer Lockbox Azure: learn.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview
• Microsoft : Customer Lockbox Power Platform (esclusione Azure OpenAI): learn.microsoft.com/en-us/power-platform/admin/about-lockbox
• Google : ISO/IEC 42001: cloud.google.com/security/compliance/iso-42001
• Google : Cloud DPA: cloud.google.com/terms/data-processing-addendum
• Google : Service Specific Terms: cloud.google.com/terms/service-terms
• Google : Data Residency GCP: cloud.google.com/terms/data-residency
• Google : Gemini Agent Platform ZDR: docs.cloud.google.com/gemini-enterprise-agent-platform/resources/zero-data-retention
• Google : Gemini Agent Platform data residency: docs.cloud.google.com/vertex-ai/generative-ai/docs/learn/data-residency
• Google : Gemini Enterprise release notes: docs.cloud.google.com/gemini/enterprise/docs/release-notes
• Google : Workspace Gemini Privacy Hub: knowledge.workspace.google.com/admin/generative-ai/generative-ai-in-google-workspace-privacy-hub
• Google : Workspace AI Privacy & Security: workspace.google.com/security/ai-privacy/
• Google : Access Transparency per Vertex AI: docs.cloud.google.com/vertex-ai/docs/general/access-transparency
• Google : Access Approval release notes: docs.cloud.google.com/assured-workloads/access-approval/docs/release-notes
• Anthropic : Certifications: privacy.claude.com/en/articles/10015870
• Anthropic : Consumer terms update: anthropic.com/news/updates-to-our-consumer-terms
• Anthropic : Data retention consumer: privacy.claude.com/en/articles/10023548
• Anthropic : Data retention commercial: privacy.claude.com/en/articles/7996866
• Anthropic : ZDR: docs.anthropic.com/en/docs/build-with-claude/zero-data-retention

• Anthropic : DPA/Commercial Terms: privacy.claude.com/en/articles/7996862
• Anthropic : Server location / data residency API: privacy.claude.com/en/articles/7996890
• Anthropic : API data residency (platform.claude.com): platform.claude.com/docs/en/manage-claude/data-residency
• Anthropic : Training data policy: privacy.claude.com/en/articles/9267385
• Anthropic : Safety/flagged content: privacy.claude.com/en/articles/10023580
• Anthropic : ZDR eligibility: privacy.claude.com/en/articles/8956058
• CNIL : Deliberazione SAN-2025-004 del 1° settembre 2025 (Google €325M): cnil.fr/en/cookies-and-advertisements-inserted-between-emails-google-fined-325-million-euros-cnil
• EDPB : Work Programme 2026-2027: edpb.europa.eu/news/edpb-work-programme-2026-2027-easing-compliance-and-strengthening-cooperation_en
• EDPB : Guidelines 03/2026 web scraping per AI generativa: edpb.europa.eu/system/files/2026-07/edpb_guidelines_2020603_webscraping_v1_en_0.pdf
• Garante italiano : Comunicato 20 dicembre 2024 (OpenAI €15M): garanteprivacy.it/home/docweb/-/docweb-display/docweb/10085432
• Catalogo ACN: acn.gov.it/portale/catalogo-delle-infrastrutture-digitali-e-dei-servizi-cloud

4. Note operative

- **Qualificazione ACN:** riguarda singole schede/servizi nel catalogo, non il provider nella sua interezza. Verificare le schede specifiche dei servizi adottati prima di ogni adozione.
- **ZDR Anthropic e contenuti flaggati:** lo ZDR non elimina la retention per contenuti flaggati dai classificatori trust & safety (2 anni input/output, 7 anni score). Vale sia per API commerciale che per consumer.
- **Flex Routing Microsoft:** per tenant EU/EFTA creati dopo il 25 marzo 2026 è abilitato di default. Verificare il setting nel Microsoft 365 admin center prima dell'adozione.
- **OpenAI EKM e apps:** con EKM abilitato le apps con funzionalità sync (ex connector) diventano non disponibili. L'ateneo deve scegliere tra gestione chiavi autonoma e integrazione con app esterne.
- **Google Gemini : distinzione prodotti:** per la PA usare solo Vertex AI Gemini o Google Workspace con Gemini in edizioni Enterprise con DPA Cloud firmato. La Gemini app consumer non è coperta da DPA aziendale.
- **Anthropic : nessuna residenza EU su API diretta:** per GDPR-compliant EU deployment obbligatorio usare AWS Bedrock EU-region o Vertex AI EU regions. L'API diretta Anthropic non offre pinning EU.
- **Shadow AI:** personale che usa account consumer (ChatGPT Free/Plus, Claude Free/Pro/Max, Gemini app gratuita) per attività lavorative espone dati istituzionali a policy di training non idonee per la PA. Per Anthropic consumer: dall'8 ottobre 2025 chi ha accettato opt-in ha retention 5 anni.
- **Raccomandazione DPO:** per uso istituzionale PA, prioritizzare provider con: (a) qualificazione ACN per i servizi specifici adottati; (b) DPA firmato con SCC nella versione corrente; (c) ZDR o retention minima con verifica delle eccezioni per contenuti flaggati; (d) CMK/BYOK compatibile con le funzionalità necessarie; (e) Access Transparency o Customer Lockbox verificando la copertura per i servizi AI specificamente adottati; (f) sub-processor list con localizzazione UE verificata; (g) DPIA completata per ogni deployment; (h) verifica Flex Routing Microsoft per tenant EU post-marzo 2026; (i) per Claude: usare AWS Bedrock EU-region o Vertex AI EU per qualsiasi requisito di residenza EU; (j) verificare che il provider abbia firmato il GPAI Code of Practice e che la documentazione tecnica art. 53 AI Act sia disponibile su richiesta.

Note metodologiche. Sezione 14 AI Act (Reg. UE 2024/1689)

Calendario applicazione AI Act (aggiornato con AI Omnibus, accordo politico 7 maggio 2026)

Le date derivanti dal Digital Omnibus on AI sono riportate sulla base dell'accordo politico del 7 maggio 2026 e dovranno essere confermate all'esito dell'adozione definitiva e della pubblicazione del regolamento modificativo.

- 2 febbraio 2025: pratiche vietate (art. 5) + AI literacy (art. 4) : APPLICABILI.
- 2 agosto 2025: obblighi provider GPAI (artt. 53 e 55): APPLICABILI. Enforcement: dal 2 agosto 2026 per nuovi modelli, dal 2 agosto 2027 per modelli già sul mercato al 2 agosto 2025.
- 2 agosto 2026: piena applicazione AI Act : sistemi ad alto rischio, trasparenza AI-generated content. Enforcement GPAI nuovi modelli.
- 2 agosto 2028: sistemi ad alto rischio embedded in prodotti regolamentati (proroga AI Omnibus).

Fonti: digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai | eur-lex.europa.eu/eli/reg/2024/1689/oj (verificate giugno 2026)

Obblighi della PA come deployer (distinti da quelli del provider)

Gli obblighi applicabili agli atenei in qualità di deployer comprendono, secondo il sistema concretamente utilizzato:

- l'adozione di misure idonee a garantire un livello sufficiente di alfabetizzazione in materia di IA del personale e degli altri soggetti che operano per loro conto;
- la verifica che l'uso previsto non integri una pratica vietata ai sensi dell'art. 5;
- per i sistemi ad alto rischio, il rispetto degli obblighi previsti dall'art. 26, inclusi l'utilizzo secondo le istruzioni, la sorveglianza umana, il monitoraggio del funzionamento e la conservazione dei log generati automaticamente quando siano sotto il controllo del deployer;
- prima del primo utilizzo, lo svolgimento della valutazione d'impatto sui diritti fondamentali prevista dall'art. 27, quando l'ateneo, quale organismo di diritto pubblico, intenda utilizzare un sistema ad alto rischio rientrante nell'art. 6, par. 2, e nell'Allegato III, punto 3, ferme restando le eccezioni previste dall'AI Act;
- ove ricorrano i presupposti, lo svolgimento della valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35 GDPR;
- per le autorità pubbliche, l'adempimento degli obblighi di registrazione nella banca dati UE previsti dall'art. 49.

GPAI Code of Practice: cosa significa per la PA

Tutti e quattro i provider del quadro (OpenAI, Google, Microsoft, Anthropic) risultano nella lista pubblica dei firmatari del GPAI Code of Practice (Commissione Europea, aggiornata al 23 aprile 2026). Questo significa che hanno dichiarato l'intenzione di adempiere agli obblighi GPAI tramite il Code of Practice, con monitoraggio dell'AI Office. Non è una certificazione di conformità: è un impegno volontario. L'enforcement con sanzioni parte dal 2 agosto 2026. Gli atenei possono richiedere ai provider la documentazione tecnica prevista dall'art. 53 (sommario dei dati di training, caratteristiche del modello).

Sovrapposizione AI Act / GDPR / NIS2

L'AI Act non modifica il GDPR né la NIS2. I tre strumenti si applicano cumulativamente. La sovrapposizione più rilevante per gli atenei: la DPIA prevista dal GDPR per trattamenti ad alto rischio coincide spesso con la valutazione d'impatto sui diritti fondamentali prevista dall'AI Act per sistemi ad alto rischio. L'EDPB e l'AI Office hanno incluso nel Work Programme 2026-2027 linee guida congiunte sull'interplay AI Act/GDPR (fonte: edpb.europa.eu, verificata giugno 2026).

Fonti verificate per la sezione 14 (AI Act)

- AI Act, Reg. UE 2024/1689: eur-lex.europa.eu/eli/reg/2024/1689/oj
- Calendario applicazione AI Act: digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
- Linee guida per provider GPAI: digital-strategy.ec.europa.eu/en/policies/guidelines-gpai-providers
- GPAI Code of Practice e lista firmatari (23 aprile 2026): digital-strategy.ec.europa.eu/en/policies/contents-code-gpai
- AI Omnibus (proposta semplificazione): eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0836
- EDPB Work Programme 2026-2027: edpb.europa.eu/system/files/2026-02/edpb_work-programme_2026-2027_en.pdf