Quadro Sinottico di Compliance NIS2/GDPR

Provider di Servizi di Intelligenza Artificiale per gli Atenei Italiani

GRUPPO ICT CRUI
Conferenza dei Rettori delle Università Italiane

Versione	1.0 — Marzo 2026
Destinatari	Rettori, Pro-Rettori delegati all'ICT, Responsabili per la Protezione dei Dati (RPD/DPO), Direzioni Generali
Autori	Gruppo ICT CRUI
Classificazione	Uso istituzionale — Diffusione consentita agli Atenei aderenti alla CRUI
Riferimenti normativi	D.Lgs. 138/2024 (NIS2); Reg. UE 2016/679 (GDPR); Reg. ACN n. 21007/24; D.Lgs. 36/2023 (Codice Appalti)

Struttura del documento

Il documento si compone dei seguenti elementi:

1. **Nota introduttiva** — illustra contesto, metodologia, perimetro e criteri di valutazione.
2. **Quadro sinottico** — tabella comparativa dei quattro provider AI (OpenAI, Google, Microsoft, Anthropic) su quindici parametri di compliance NIS2/GDPR.
3. **Allegato 1 — Amazon Web Services / Amazon Bedrock** — analisi separata di AWS Bedrock come layer infrastrutturale di distribuzione dei modelli AI, con motivazione della classificazione distinta e valutazione degli stessi quindici parametri.

1. Nota introduttiva — Metodologia, perimetro e criteri di valutazione

1.1 Contesto e origine del documento

La rapida diffusione, nel corso del 2025, dei servizi di intelligenza artificiale generativa ha posto il sistema universitario italiano di fronte a esigenze nuove e urgenti, che i tradizionali cicli di procurement pubblico non sempre riescono ad assorbire con la necessaria rapidità. Chatbot, assistenti alla ricerca, strumenti di supporto alla didattica, sistemi di analisi documentale: in pochi mesi queste soluzioni sono passate dall'essere oggetto di sperimentazione accademica a essere utilizzate, spesso in modo non governato, da docenti, ricercatori, personale tecnico-amministrativo e studenti, spesso mediante account personali e senza alcuna valutazione preliminare della conformità normativa.

Il Gruppo ICT della CRUI ha raccolto, nell'ambito delle interlocuzioni con i Rettori e con i Delegati ICT degli Atenei aderenti, l'esigenza di disporre di un quadro di valutazione sistematico e giuridicamente fondato in ordine all'adottabilità, da parte delle università italiane, dei principali servizi di intelligenza artificiale commerciali.

Tale quadro risponde, in primo luogo, all'esigenza della stazione appaltante di disporre di una base istruttoria omogenea a supporto della predisposizione dei capitolati di gara, della definizione dei requisiti contrattuali e della costruzione di una cornice comune di valutazione dei rischi. Resta fermo, tuttavia, che la valutazione finale di adottabilità e di rischio in concreto compete ai singoli Atenei, in qualità di soggetti utilizzatori e titolari dei trattamenti, dovendo essa necessariamente misurarsi con variabili ulteriori, quali la tipologia di dati trattati, i casi d'uso previsti, il livello di integrazione del servizio nei processi istituzionali, il contesto tecnologico di riferimento e le misure organizzative e tecniche concretamente adottate.

L’esigenza non si presenta in termini generici, ma trae origine da specifiche necessità operative e dai peculiari vincoli ordinamentali, organizzativi e tecnologici che caratterizzano il sistema universitario, tra cui:

- la necessità di mettere a disposizione dei Responsabili della protezione dei dati e degli uffici competenti una base documentale utile ai fini delle valutazioni preliminari di impatto, dell’aggiornamento del registro dei trattamenti e, più in generale, della verifica di conformità al quadro europeo e nazionale in materia di protezione dei dati personali; la redazione di DPIA e per l'aggiornamento del Registro dei Trattamenti;
- l’urgenza di tenere conto dell’entrata in vigore del d.lgs. 138/2024, di recepimento della direttiva NIS2, che ha esteso in modo significativo gli obblighi in materia di sicurezza informatica anche alle università, qualificate come soggetti importanti ai sensi dell’art. 3, comma 1, lett. b), del decreto;
- la necessità di offrire agli organi di governo degli Atenei e alle strutture tecnico-amministrative uno strumento comune, idoneo a ridurre la frammentazione delle analisi, a favorire valutazioni comparabili e a rafforzare l’uniformità metodologica delle decisioni;
- l’opportunità di disporre di un supporto istruttorio che consenta di distinguere, già in fase di procurement, tra profili suscettibili di standardizzazione a livello di stazione appaltante e profili che, invece, richiedono una successiva declinazione da parte dei singoli Atenei in relazione ai rispettivi assetti organizzativi, ai trattamenti effettuati e ai livelli di rischio concretamente riscontrabili;
- la necessità, infine, di accompagnare l’introduzione dei sistemi di IA con un approccio di procurement consapevole, capace di integrare, sin dalla fase di affidamento, le esigenze di conformità giuridica, sicurezza, governance del dato, sostenibilità organizzativa e controllabilità del fornitore.

Il presente documento costituisce la nota introduttiva al Quadro Sinottico di compliance NIS2/GDPR di Provider AI e ne illustra il perimetro, la metodologia, le scelte classificatorie e i limiti. Il Quadro stesso è concepito come strumento di lavoro a uso istituzionale, non come parere legale né come valutazione vincolante ai fini dell’adozione degli strumenti di AI: resta responsabilità di ciascun Ateneo condurre le verifiche specifiche e, ove necessario, la DPIA di cui all'art. 35 GDPR.

1.2. Perimetro della valutazione: cosa è stato analizzato e cosa no

1.2.1 I provider inclusi nel Quadro Sinottico

Il Quadro Sinottico analizza i seguenti quattro fornitori di servizi AI nella loro veste di erogatori del modello linguistico:

- **OpenAI** (ChatGPT Enterprise / API Platform) — modello GPT-4o e successivi;
- **Google** (Gemini for Workspace Enterprise / Vertex AI) — modello Gemini 1.5 Pro e successivi;
- **Microsoft** (Azure OpenAI Service) — accesso ai modelli OpenAI tramite infrastruttura Microsoft Azure;
- **Anthropic** (Claude Enterprise / API) — modello Claude 3 e 4.

Il perimetro è circoscritto ai piani enterprise e alle modalità di accesso tramite API, che sono le uniche modalità di utilizzo compatibili con i requisiti di una stazione appaltante pubblica. I piani consumer (ChatGPT Free, ChatGPT Plus, Gemini personale, Claude Free e Claude Pro) sono esplicitamente esclusi dalla valutazione: le condizioni contrattuali consumer non soddisfano i requisiti minimi del GDPR per il trattamento di dati personali in ambito professionale, non prevedono un DPA ai sensi dell'art. 28 GDPR e, come dimostrato dalle modifiche alle policy

Anthropic del settembre 2025, espongono i dati inseriti dagli utenti a utilizzo per il training del modello. Il loro utilizzo da parte di personale universitario per attività istituzionali che coinvolgano dati personali o dati riservati costituisce una violazione del GDPR a carico dell'Ateneo nella sua veste di titolare del trattamento.

Nota sulla protezione dei dati — Rischio shadow AI
L'uso di account consumer personali da parte di dipendenti universitari per svolgere attività istituzionali è una delle principali fonti di esposizione al rischio in questo ambito. Ai sensi dell'art. 28 GDPR, il titolare del trattamento risponde dei trattamenti effettuati per suo conto anche se eseguiti mediante strumenti non formalmente autorizzati. E' fortemente raccomanda l'adozione di una policy BYOA (Bring Your Own AI) che identifichi gli strumenti approvati e i requisiti minimi di accesso, e la relativa comunicazione al personale.

1.2.2 Amazon Web Services / Amazon Bedrock: perché in allegato e non in tabella

Una scelta metodologica che richiede esplicitazione riguarda il motivo per cui Amazon Web Services (AWS), e in particolare Amazon Bedrock, non figurano come quinta colonna del Quadro sinottico, ma sono trattati separatamente nell'Allegato 1.

I quattro provider inclusi nel Quadro sinottico sono stati selezionati in quanto fornitori del modello di AI, ossia soggetti che sviluppano, addestrano, controllano e governano il modello linguistico. Il criterio adottato per la redazione del Quadro sinottico non è, pertanto, quello del soggetto che mette a disposizione l'infrastruttura cloud o il layer tecnico di erogazione del servizio, ma quello del soggetto che controlla il modello e il servizio di AI oggetto di analisi.

I fornitori dell'infrastruttura o delle piattaforme di distribuzione restano naturalmente rilevanti sotto altri profili, ma tali aspetti non costituiscono, in questa sede, il parametro seguito per individuare i provider oggetto della comparazione.

In tale prospettiva, AWS è stato esaminato separatamente in allegato, in ragione di una specifica richiesta formulata dalla Commissione ICT CRUI. La scelta risponde anche a un'esigenza di correttezza classificatoria: Amazon Bedrock costituisce un distinto layer di erogazione e accesso ai modelli, attraverso il quale possono essere resi disponibili modelli di terzi, inclusi quelli di Anthropic, secondo opzioni regionali e geografiche che incidono sul profilo di compliance del servizio. Una sua collocazione nella medesima tabella principale, accanto ai provider selezionati come fornitori del modello, avrebbe pertanto sovrapposto piani di analisi non perfettamente omogenei.

Per tale ragione, AWS/Bedrock è stato oggetto di trattazione separata nell'Allegato 1, costruito secondo la medesima struttura parametrica del Quadro sinottico, così da consentire una lettura coordinata, ma mantenendo distinta la valutazione del provider del modello da quella del layer infrastrutturale e di distribuzione attraverso cui il servizio può essere concretamente fruito.

Resta fermo che il presente Quadro sinottico non ha finalità esaustiva rispetto a tutti i cloud service provider, alle piattaforme di distribuzione o ai canali di erogazione attraverso cui i modelli di AI possono essere resi disponibili. Esso rappresenta, invece, una comparazione selettiva costruita secondo un criterio metodologico puntuale, limitato ai quattro provider del modello individuati. Eventuali ulteriori soggetti rilevanti sul piano infrastrutturale o distributivo possono essere oggetto di analisi dedicata, ove ciò sia richiesto.

1.3. Metodologia

1.3.1 Fonti utilizzate

La valutazione si basa esclusivamente su documentazione pubblica ufficiale dei provider alla data di marzo 2026:

- Data Processing Addendum (DPA) e termini contrattuali enterprise;
- pagine di privacy e sicurezza pubblicate sui siti istituzionali dei provider;
- documentazione tecnica (Trust Center, whitepapers di sicurezza);
- catalogo ACN delle infrastrutture e dei servizi cloud qualificati;
- normativa primaria e secondaria italiana ed europea.

Non sono state utilizzate dichiarazioni commerciali, materiali di marketing o fonti secondarie non verificabili.

La ricerca è stata condotta su tutti e quattro i provider con il medesimo protocollo di interrogazione, al fine di garantire comparabilità. Laddove un'informazione non era reperibile nella documentazione pubblica ufficiale, il parametro è stato valutato come "non dichiarato".

1.3.2 Aggiornamento e obsolescenza

Le policy dei provider AI si modificano con frequenza elevata e talvolta senza preavviso adeguato. Il caso più emblematico documentato nel corso della presente analisi è quello di Anthropic, che nel settembre 2025 ha modificato radicalmente le condizioni di utilizzo per gli account consumer, introducendo il training sui dati degli utenti come modalità di default (opt-out).

Parallelamente, Microsoft ha rimosso dalla documentazione pubblica di Azure OpenAI il riferimento esplicito alla finestra di retention di 30 giorni per l'abuse monitoring, generando un'ambiguità documentale che le stazioni appaltanti sono costrette a segnalare nelle proprie procedure di due diligence.

Il presente Quadro è pertanto da intendersi come strumento a validità temporanea.

Si raccomanda una revisione semestrale, con verifica sistematica dei DPA e delle policy di ciascun provider. La data di riferimento della presente versione è marzo 2026.

1.4. I parametri di valutazione: perché questi quindici ambiti

I quindici parametri del Quadro non sono stati selezionati in modo arbitrario né per mera somiglianza con checklist di compliance generiche. Ciascun parametro risponde a una specifica esigenza del sistema universitario italiano, derivante dalla congiunzione di tre quadri normativi obbligatori (GDPR, NIS2 e Strategia Cloud Italia/qualificazione ACN) e dalla natura peculiare del trattamento dei dati in contesto universitario.

Il Quadro non esprime un giudizio di idoneità complessiva dei provider. L'idoneità dipende dalla classificazione dei dati trattati dall'Ateneo (dati ordinari, critici o strategici ai sensi della Strategia Cloud Italia), dalla tipologia di utilizzo prevista e dalla configurazione specifica del servizio. Un provider che presenta una valutazione su un parametro può essere idoneo per un utilizzo a basso rischio e non idoneo per un utilizzo che coinvolge dati sensibili o critici.

Di seguito la motivazione analitica per ciascun parametro:

N.	Parametro di valutazione	Motivazione per il sistema universitario italiano
1	**Qualificazione ACN dell'infrastruttura cloud**	Il D.Lgs. 138/2024 (NIS2) impone alle università di verificare la sicurezza della supply chain ICT. La Strategia Cloud Italia (Reg. ACN n. 21007/24) richiede che le PA acquistino servizi cloud esclusivamente da fornitori qualificati ACN. Senza la verifica della qualifica, l'adozione del servizio

N.	Parametro di valutazione	Motivazione per il sistema universitario italiano
		è di per sé non conforme alla normativa di settore per la PA, indipendentemente da qualsiasi altra considerazione.
2	**Certificazione ISO/IEC 27001**	La qualifica ACN di livello 1 richiede la certificazione ISO 27001 (o CSA STAR Level 2 in alternativa) come condizione necessaria. Per l'Ateneo che valuta il servizio è il primo indicatore di maturità del sistema di gestione della sicurezza delle informazioni del fornitore, indipendentemente dal sistema di qualificazione ACN.
3	**Conformità GDPR**	Le università trattano categorie particolari di dati (dati sanitari degli studenti con disabilità, dati giudiziari, dati biometrici per l'accesso ai laboratori, dati sanitari per motivi di ricerca ecc.) e sono titolari di trattamenti ad alto rischio. Il GDPR è l'asse normativo primario di valutazione. La conformità GDPR è valutata in modo distinto dagli altri parametri perché copre aspetti di governance contrattuale (DPA, SCC, entità contrattuale UE) che sono precondizioni per qualsiasi altro giudizio di compliance.
4	**Divieto di uso dei dati per il training**	Nelle università transitano dati di ricerca riservata (pre-pubblicazione), elaborati di tesi, dati sperimentali, corrispondenza con studenti contenente dati personali sensibili. L'utilizzo di tali dati per il training del modello del fornitore costituirebbe una violazione del GDPR (assenza di base giuridica, finalità incompatibile) e un rischio per la proprietà intellettuale dell'Ateneo. Il parametro è disaggregato per coprire anche le forme indirette di utilizzo (debug, quality evaluation, monitoring), che nella pratica costituiscono la principale area grigia contrattuale.
5	**Residenza dei dati in UE**	Il GDPR limita il trasferimento di dati personali verso paesi terzi non adeguati. La Strategia Cloud Italia richiede che i dati della PA siano mantenuti nell'UE. Per le università, la residenza EU è particolarmente rilevante per i dati degli studenti, per i dati di ricerca finanziata con fondi pubblici, e per i dati relativi a procedure concorsuali e amministrative (la lista è esemplificativa e non esaustiva). Il parametro analizza separatamente storage at-rest, inference in-region e accesso da personale UE, in quanto le tre dimensioni possono essere soddisfatte in modo disgiunto dai provider.
6	**Descrizione del logging**	La NIS2 richiede che le organizzazioni mantengano capacità di rilevamento degli incidenti e di tracciabilità degli accessi ai sistemi informativi critici. Ai fini GDPR, la tracciabilità dei trattamenti è parte dell'accountability.
7	**Logging e audit esportabili**	La possibilità di esportare i log in formato strutturato verso sistemi SIEM è un requisito operativo diretto della NIS2 (art. 21 della Direttiva, recepito nell'art. 24 D.Lgs. 138/2024), che impone misure per il monitoraggio, la registrazione e la rilevazione degli incidenti. Per gli Atenei che hanno adottato SOC interni o in outsourcing, la non esportabilità dei log rende impossibile l'integrazione del servizio AI nel perimetro di monitoraggio della sicurezza.
8	**Retention di prompt, dati e log**	Questo parametro è deliberatamente tenuto distinto dal parametro 4 (no training) per le seguenti ragioni: un provider può dichiarare di non usare i dati per il training e tuttavia conservarli per 30 giorni nei log di abuse monitoring, esponendoli potenzialmente ad accessi da personale interno o a richieste di autorità straniere. Per le Università, la configurabilità della retention è un requisito di minimizzazione ai sensi dell'art. 5, par. 1, lett. e) GDPR e di proporzionalità ai fini NIS2.
9	**Cifratura in transito e a riposo**	Standard di base NIS2/GDPR. Rilevante per le università perché la cifratura deve coprire tutti i componenti del sistema (log, cache, telemetria, sistemi di abuse monitoring) e non soltanto il canale principale cliente-server. La dichiarazione generica di cifratura AES-256/TLS non è sufficiente: il parametro valuta la granularità della dichiarazione.
10	**Gestione delle chiavi crittografiche (BYOK/CMK)**	Il modello BYOK (Bring Your Own Key) è il requisito minimo per garantire che l'Ateneo mantenga controllo effettivo sui propri dati anche in caso di compromissione del fornitore o di ordine di divulgazione emesso da un'autorità straniera. Per le università con dati di ricerca classificati o finanziati da soggetti con particolari requisiti di sicurezza (difesa, sanità, brevetti), BYOK è condizione necessaria per il deployment.
11	**Controllo degli accessi privilegiati del fornitore**	La NIS2 richiede la gestione del rischio connesso all'accesso di terze parti ai sistemi. Il rischio non è solo esterno (attaccanti) ma interno (personale del fornitore con accesso privilegiato). Per le Università, che essendo pubbliche amministrazioni, per il principio di trasparenza sono esposte a

N.	Parametro di valutazione	Motivazione per il sistema universitario italiano
		maggiori obblighi di accountability, la conoscenza di chi può accedere ai dati lato fornitore è requisito per la redazione della DPIA e per la valutazione del rischio residuo.
12	**Gestione degli incidenti e notifica violazioni**	Il GDPR (art. 33) impone la notifica al Garante entro 72 ore dalla conoscenza di una violazione dei dati personali. La NIS2 (art. 23 Direttiva, art. 25 D.Lgs. 138/2024) estende obblighi analoghi agli incidenti di sicurezza significativi. Per l'Ateneo che ha esternalizzato il trattamento a un provider AI, la capacità di rispettare questi termini dipende in modo critico dalla tempestività con cui il provider notifica l'incidente al cliente. Il parametro valuta le procedure dichiarate e le tempistiche contrattualmente garantite.
13	**Minimizzazione dei dati nei sistemi di monitoring**	La minimizzazione (art. 5, par. 1, lett. c) GDPR) si applica a tutti i componenti del sistema, inclusi i log di abuse monitoring, i sistemi di telemetria e le cache di latenza. Il parametro è inserito autonomamente, pur essendo in parziale sovrapposizione con i parametri 4 e 8, perché risponde a un rischio specifico del sistema universitario: il logging del contenuto integrale dei prompt (che può contenere dati personali di studenti, dati di ricerca riservata, corrispondenza istituzionale) nei sistemi di monitoring del fornitore, anche in assenza di utilizzo per il training.
14	**Gestione dei sub-fornitori (supply chain)**	La NIS2 (art. 21, par. 2, lett. d) Direttiva) richiede che le organizzazioni adottino misure per la sicurezza della catena di approvvigionamento, inclusa la verifica dei sub-fornitori. Per le Università, la mancata dichiarazione dell'elenco dei sub-fornitori (art. 28, par. 3, lett. d) GDPR) rende impossibile valutare il rischio di trasferimento dati verso paesi terzi tramite sub-fornitori e impedisce la redazione di una DPIA completa.
15	**Isolamento tra tenant**	Le Università condividono l'infrastruttura del provider con decine di migliaia di altri clienti, incluse potenzialmente altre PA, aziende private, soggetti esteri. L'isolamento logico e fisico tra tenant è il requisito minimo per escludere la possibilità di contaminazione dei dati tra clienti diversi. La certificazione di tale isolamento da parte di auditor indipendenti (SOC 2 Type 2, ISO 27001) è l'unico strumento di verifica disponibile per la stazione appaltante che non può condurre audit diretti sull'infrastruttura del fornitore.

1.5. Avvertenze operative

1.5.1 Il Quadro non sostituisce la due diligence delle amministrazioni

Il presente strumento è pensato per orientare la valutazione preliminare e per identificare i punti critici da approfondire nella fase di negoziazione contrattuale. Non sostituisce la lettura diretta e aggiornata del DPA del provider, né l'esame delle condizioni specifiche del piano enterprise prescelto.

1.5.2 La qualificazione ACN riguarda il CSP, non il servizio AI applicativo

Merita, inoltre, una precisazione il tema della qualificazione ACN, spesso oggetto di equivoci interpretativi. La qualificazione ACN non riguarda esclusivamente il layer infrastrutturale cloud (IaaS/PaaS), ma può estendersi anche a specifici servizi cloud qualificati e pubblicati nel Catalogo dei servizi cloud per la PA. Ciò non comporta, tuttavia, che la qualificazione dell'infrastruttura o di servizi cloud di base determini automaticamente la qualificazione del singolo servizio di intelligenza artificiale applicativo o SaaS che su tale infrastruttura si appoggia.

Allo stato, con riferimento ai principali servizi AI commerciali qui considerati, non risulta evidenza pubblica di una qualificazione ACN specifica, con tale denominazione commerciale, per servizi quali ChatGPT Enterprise, Claude, Gemini for Workspace o Azure OpenAI. Ne consegue che l'eventuale qualificazione del cloud sottostante costituisce certamente un elemento rilevante ai fini istruttori, ma non è, di per sé, sufficiente a fondare un giudizio di piena adottabilità del servizio AI.

La verifica deve pertanto essere completata dal singolo Ateneo in relazione alla classificazione dei dati e dei servizi coinvolti, alla tipologia di utilizzo prevista, al livello di integrazione del servizio nei processi istituzionali, nonché

alle misure tecniche, organizzative e contrattuali effettivamente applicabili. In questa prospettiva, la qualificazione del layer infrastrutturale o dei servizi cloud di base rappresenta una condizione favorevole e, in taluni casi, necessaria, ma non assorbe né sostituisce la valutazione sostanziale del rischio e della conformità del servizio AI concretamente acquisito.

1.5.3 Scadenza delle qualifiche

Le qualifiche rilasciate nel regime transitorio antecedente all'entrata in applicazione del Regolamento ACN n. 21007/24 presentavano, nei casi previsti dal relativo decreto, una validità di dodici mesi dalla data di concessione. Le qualifiche rilasciate ai sensi del Regolamento ACN n. 21007/24, applicabile dal 1° agosto 2024, hanno invece durata massima di trentasei mesi. Con riferimento alle schede ACN di Google Cloud Italy S.r.l. esaminate nel presente documento, eventuali date di scadenza rilevate in sede di analisi devono essere considerate suscettibili di aggiornamento o rinnovo alla data di pubblicazione. La stazione appaltante verifica la validità delle qualifiche in fase di stipula del contratto. Ciascun Ateneo è comunque tenuto a verificare direttamente lo stato aggiornato delle schede presenti nel Catalogo ACN prima di procedere all'adozione del servizio.

2 Quadro sinottico

2.1 Tabella comparativa dei quattro provider AI (OpenAI, Google, Microsoft, Anthropic) su quindici parametri di compliance NIS2/GDPR

La valutazione è condotta ai fini della compliance con la Direttiva NIS2 (D.Lgs. 138/2024) e il GDPR (Reg. UE 2016/679), con particolare riferimento ai requisiti di sicurezza della catena di approvvigionamento e alla qualificazione ACN ai sensi del Reg. n. 21007/24.

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

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 ufficiale: https://www.acn.gov.it/portale/catalogo-delle-infrastrutture-digitali-e-dei-servizi-cloud				
1.1 Qualificazione ACN infrastruttura cloud	Non qualificata* OpenAI non ha qualificazione ACN propria; accessibile via Azure OpenAI (infrastruttura Microsoft) *in corso la valutazione delle risorse legali e operative per ottenere la qualificazione ACN Fonti: Catalogo ACN ufficiale: https://www.acn.gov.it/portale/catalogo-delle-	Livello 2 (QC2/QI2) Google Cloud ha ottenuto qualifica ACN Livello 2 per dati ordinari e critici, infrastruttura e servizi Workspace/GCP Fonti: Catalogo ACN ufficiale: https://www.acn.gov.it/portale/catalogo-delle-infrastrutture-digitali-e-dei-servizi-cloud	Tramite PSN / Catalogo ACN Azure qualificato ACN per dati ordinari/critici. Livello di qualificazione 2 Microsoft Azure è presente nel catalogo ACN tramite il Polo Strategico Nazionale (PSN) con Secure Public Cloud IaaS/PaaS. Fonti: Catalogo ACN ufficiale: https://www.acn.gov.it/portale/catalogo-delle-infrastrutture-digitali-e-dei-servizi-cloud	Non qualificata Anthropic non ha qualificazione ACN propria. Claude accessibile via AWS Bedrock o Azure (infrastruttura del CSP), su cui ricade la qualifica. Ma la fruizione del modello tramite CSP qualificato rileva in termini infrastrutturali e di sicurezza, ma non estende automaticamente la qualifica al servizio di IA, che richiede autonoma valutazione da parte della PA. Fonti: Catalogo ACN ufficiale: https://www.acn.gov.it/porta

Ambito di valutazione	OpenAI (ChatGPT Ent./API)	Google (Gemini / Vertex AI)	Microsoft (Azure OpenAI)	Anthropic (Claude Ent./API)
	infrastrutture-digitali-e-dei-servizi-cloud			le/catalogo-delle-infrastrutture-digitali-e-dei-servizi-cloud
1.2 ISO/IEC 27001	Certificata ISO 27001 ISO 27017 ISO 27018 ISO 27701 + SOC 2 Type 2 + CSA STAR OpenAI Trust Portal: https://trust.openai.com	Certificata ISO 27001 ISO 27017 ISO 27018 ISO 27701 ISO 42001 + SOC 1/2/3 + FedRAMP High Vertex AI Security Controls: documentazione ufficiale Google Cloud https://cloud.google.com/security/compliance •	Certificata ISO 27001 ISO 27017 ISO 27018 + SOC 1/2 + FedRAMP + HIPAA BAA. Azure tra i più estesi portfolio di compliance Microsoft Trust Center: https://www.microsoft.com/trust-center • Microsoft Learn: Azure compliance offerings	Certificata ISO 27001 + SOC 2 Type 2. Portfolio certificativo più limitato rispetto a hyperscaler. L'infrastruttura sottostante AWS/Azure eredita le loro certificazioni Anthropic Trust Center: https://trust.anthropic.com • Privacy Center: https://privacy.claude.com
2. Conformità GDPR				
2.1 DPA (Data Processing Addendum) conforme art. 28 GDPR	Disponibile DPA con SCC per trasferimenti extra-UE. Entità contrattuale UE: OpenAI Ireland Ltd https://openai.com/policies/data-processing-addendum • Google Cloud DPA	Disponibile Cloud DPA aggiornato GDPR; SCC incorporate. Entità contrattuale UE: Google Ireland Ltd https://cloud.google.com/terms/data-processing-addendum	Disponibile Microsoft DPA completo con SCC; framework EU-US DPF; Entità contrattuale UE: Ireland Operations Ltd https://aka.ms/DPA	Disponibile DPA con SCC disponibile per clienti commerciali/enterprise. NOTA: l'integrazione Claude in M365 Copilot attualmente è esclusa dall'EU Data Boundary Microsoft (da verificare aggiornamenti) https://www.anthropic.com/legal/dpa
2.2 Diritti dell'interessato (accesso, cancellazione, portabilità)	Supportato - Privacy Center self-service; - supporto DSR; - cancellazione propagata entro	Supportato - Admin console Workspace; - DSR via Google Cloud; - accesso, cancellazione, portabilità garantiti	Supportato - Microsoft Trust Center; - richieste DSR tramite admin portal;	Supportato - Privacy Center Anthropic; - DSR gestibili;

Ambito di valutazione	OpenAI (ChatGPT Ent./API)	Google (Gemini / Vertex AI)	Microsoft (Azure OpenAI)	Anthropic (Claude Ent./API)
	30 gg dalla richiesta		- SLA di risposta dichiarate	- cancellazione chat entro 30 gg nei log di back-end
2.3 Base giuridica del trattamento dichiarata	Parziale Dichiarata (esecuzione contratto + legittimo interesse). Sanzione Garante: €15M dic.2024 per assenza base giuridica su utenti consumer. Enterprise: più chiaro	Dichiarata Esecuzione contratto / legittimo interesse. Politica opt-in esplicita per GDPR (es. Gmail Personal Intelligence richiede opt-in in UE)	Dichiarata Contratto + legittimo interesse; quadro legale solido DPA/SCC	Dichiarata Contratto + legittimo interesse per account enterprise/API. Consumer: modifica set. 2025 ha introdotto opt-in training
3. Divieto uso dati per training (incluso debug/qualità)				
3.1 Esclusione training su dati cliente (enterprise/API)	Garantita per API/Enterprise Per API e piani business nessun uso per training salvo opt-in esplicito. Consumer Free/Plus: training abilitato di default (opt-out possibile) 'By default, we do not use data from ChatGPT Enterprise, ChatGPT Business, ChatGPT Edu, ChatGPT for Healthcare, ChatGPT for Teachers, or our API platform—including inputs or outputs—for training or improving our models.' https://openai.com/business-data/ (Business Data Privacy) • https://openai.com/enterprise-privacy/	Garantita per Vertex AI / Workspace Enterprise Service Specific Terms: Google non usa dati cliente per training senza permesso esplicito. Consumer gemini.google.com: possibile uso per improvement https://services.google.com/fh/files/misc/genai_privacy_google_cloud_20230 8.pdf •	Garantita Prompts e completions Azure OpenAI non condivisi con OpenAI né usati per training Microsoft/OpenAI. Dichiarazione contrattuale esplicita nei Product Terms https://learn.microsoft.com/en-us/azure/foundry/responsible-ai/openai/data-privacy	Garantita per API/Enterprise API: nessun uso per training, policy flat. Enterprise/Gov/Education: esclusi per contratto. Consumer set. 2025: opt-in training (chi non ha optato out, incluso nei dati di training) Aggiungere nota esplicita nel quadro sulla 'shadow AI' – dipendenti che usano account personali per attività lavorative. Questa è una vulnerabilità reale per le università. https://privacy.claude.com/en/articles/7996868

Ambito di valutazione	OpenAI (ChatGPT Ent./API)	Google (Gemini / Vertex AI)	Microsoft (Azure OpenAI)	Anthropic (Claude Ent./API)
3.2 Esclusione uso per debug / valutazione qualità / monitoring interno	Parziale / Non esplicita Abuse monitoring automatico dichiarato; possibile revisione umana limitata per sicurezza. ZDR (zero data retention) disabilita storage. Non dichiarazione esplicita su esclusione debug indiretto https://openai.com/it-IT/policies/services-agreement/	Parziale Vertex AI: in-memory cache 24h TTL per latenza (disabilitabile). Abuse monitoring in-region. Workspace: no human review senza consenso. ZDR disponibile ma richiede disabilitazione cache + opt-out abuse logging https://cloud.google.com/terms	Condizionato a configurazione Abuse monitoring automatico in-region (EU) per deployment EU. Human review da personale EU. Possibile disabilitare log storage abuse con approvazione Microsoft. Non esclusione esplicita debug su tutti i componenti https://azure.microsoft.com/en-us/support/legal/	Parziale API log 7 gg default (da set. 2025); ZDR disponibile per enterprise qualificati. Non esclusione esplicita e completa di qualsiasi forma di debug/monitoring su tutti i percorsi dati interni https://openai.com/it-IT/policies/services-agreement/
4. Residenza dei dati in UE (trattamento, memorizzazione, accesso)				
4.1 Data residency UE (at-rest storage)	Disponibile (Enterprise/API) Data residency EU per ChatGPT Enterprise, Edu, API. Dati a riposo nei data center europei https://openai.com/business-data/ (sezione 'We offer data residency')	Disponibile Vertex AI: regioni EU selezionabili. Workspace: EU data region configurabile. Opzione EU-only per elaborazione e storage https://docs.cloud.google.com/vertex-ai/generative-ai/docs/learn/data-residency	Disponibile con EU DataZone EU Data Zone Standard garantisce input/output/log in Europa. Deployment Global Standard: i dati possono uscire dall'UE – non conforme GDPR per PII https://learn.microsoft.com/en-us/azure/foundry/responsible-ai/openai/data-privacy	Dipende dal deployment Anthropic API diretto: infrastruttura AWS US. Via AWS Bedrock EU o Azure EU region: residenza garantita dal CSP. Nessuna garanzia EU-only nativamente sul prodotto Anthropic diretto Anthropic non gestisce infrastruttura EU propria.
4.2 Elaborazione (inference) in-region UE	Disponibile (opt-in, EU GPU inference) Lanciata ad apr. 2025 per Enterprise/Edu: GPU inference in-region EU. Da configurare esplicitamente https://openai.com/business-data/ (sezione 'data retention controls')	Disponibile Vertex AI: regioni EU supportate per inference. Workspace: elaborazione EU configurabile https://docs.cloud.google.com/vertex-ai/generative-ai/docs/vertex-ai-zero-data-retention	EU DataZone / Regional Standard Con EU DataZone o Regional Standard EU: inference garantita in-region. Global Standard: inference globale (no garanzia EU) https://azure.microsoft.com/it-it/explore/global-infrastructure/data-residency#:~:text=Reside	Solo via CSP di supporto Inference EU garantita solo se erogato via AWS Bedrock EU-region o Azure EU. Prodotto diretto: infrastruttura USA

Ambito di valutazione	OpenAI (ChatGPT Ent./API)	Google (Gemini / Vertex AI)	Microsoft (Azure OpenAI)	Anthropic (Claude Ent./API)
			nza%20dei%20dati%20in%20Azure%20%7C%20Microsoft%20Azure.	
4.3 Accesso ai dati limitato a personale UE	Non dichiarato esplicitamente Sede US; DPA impone SCC ma non restringe geograficamente l'accesso operativo del personale a UE	Parziale Workspace: abuse monitoring human review riservato a personale EU quando tenant EU. Non dichiarazione completa su tutti i componenti	Parzialmente garantito Azure EU Data Boundary: accesso supporto limitato a EU/EEA. Data Guardian (opzione sovereign cloud) per approvazione accessi da personale extra-UE	Non dichiarato Sede USA; nessuna restrizione geografica esplicita sul personale con accesso operativo
5. Logging: contenuto, dettaglio e configurabilità				
5.1 Descrizione contenuto log (cosa viene registrato)	Parziale Input/output registrati per abuse monitoring. ZDR elimina storage ma non il processing momentaneo. Metadati (timestamp, token count, model) sempre registrati	Parziale Vertex AI: log standard Cloud Logging (metadati richiesta, latenza, token). Contenuto prompt/completion registrato per abuse; disabilitabile. ZDR: nessuna persistenza	Documentato Azure Monitor / Azure OpenAI: metadati request, token usage, latenza, content filtering risultati. Prompts e completions loggati per abuse (disabilitabile con approvazione). Dettaglio configurabile	Limitata documentazione pubblica API log: 7 gg default; input/output inclusi. ZDR: nessuna persistenza oltre il necessario. Documentazione pubblica granulare sul contenuto dei log non dettagliata
5.2 Log e audit esportabili	Limitato Usage dashboard disponibile. Export strutturato log per audit non dichiarato come feature nativa; dipende da integrazione SIEM del cliente	Disponibile Cloud Audit Logs esportabili verso BigQuery, SIEM. Workspace Admin: audit log export CSV/API. Strutturato e scalabile	Disponibile Azure Monitor / Log Analytics: export SIEM (Sentinel, Splunk), EventHub, Storage. Audit log completi e strutturati per Azure OpenAI	Limitato (nativamente) Via AWS Bedrock: CloudTrail + CloudWatch export. Via API diretta: nessun export nativo strutturato dichiarato. Dipende fortemente dal layer infrastrutturale
6. Politiche di retention di prompt, dati e log (dichiarata e configurabile)				

Ambito di valutazione	OpenAI (ChatGPT Ent./API)	Google (Gemini / Vertex AI)	Microsoft (Azure OpenAI)	Anthropic (Claude Ent./API)
6.1 Retention log e prompt (default)	**Dichiarata e configurabile** Enterprise/API: retention configurabile; ZDR disponibile (nessuna persistenza). Default: 30 gg per piani business. Log abuse monitoring: temporanei	**Dichiarata** Vertex AI ZDR: nessuna persistenza prompt/completion. Default: log Cloud Logging 30 gg (configurabile). Cache in-memory 24h TTL (disabilitabile)	**Dichiarata e configurabile** Default: prompts/completions non conservati dopo la risposta (salvo abuse monitoring temporaneo). Admin può configurare retention; ZDR su richiesta. Da giugno 2025: admin console retention controls	**Dichiarata e in miglioramento** API: da setttembre 2025 log 7 gg (ridotto da 30). ZDR disponibile per enterprise qualificati. Enterprise può optare per 30 gg via DPA per audit. Consumer: 30 gg o 5 anni (se opt-in training)
6.2 Separazione tra retention operativa dei log e uso per training	**Attenzione** ZDR elimina retention ma non è disponibile su tutti i piani. Senza ZDR: log abuse monitoring (temporanei, non per training) vs. dati customer (non per training su enterprise). Rischio: impiego di log per debug non esplicitamente escluso	**Attenzione su abuse log** Vertex AI: cache e abuse log sono distinti dai dati di training. Per ZDR pieno: necessario disabilitare cache + opt-out abuse logging-Separazione non automatica	**Documentata** Abuse monitoring log separati e temporanei; non usati per training. Disabilitabile con approvazione. Documentazione su separazione tra operational log e training data più esplicita rispetto ad altri	**Parziale** API log 7 gg: non usati per training (dichiarato). Tuttavia: esclusione esplicita dall'uso per debug/quality evaluation indiretto non completamente documentata per tutti i percorsi
7. Cifratura dati in transito e a riposo (tutti i componenti)				
7.1 Cifratura in transito	**TLS 1.2+ dichiarato** TLS 1.2+ tra cliente e OpenAI e tra OpenAI e sub-fornitori. Dichiarazione esplicita	**TLS 1.3 dichiarato** TLS per tutte le comunicazioni verso e internamente a Google Cloud. Standard Google Cloud applicato	**TLS 1.2+ dichiarato** TLS per tutte le comunicazioni cliente-Azure e componenti interni. Standard Azure applicato uniformemente	**TLS dichiarato** Comunicazioni cifrate in transito. Dettaglio versione TLS e copertura componenti interni non completamente documentata pubblicamente
7.2 Cifratura a riposo (inclusi log, cache, audit)	**AES-256 dichiarato** AES-256 per dati a riposo inclusi i dati cliente. EKM (Enterprise Key Management) disponibile per chiavi proprie del cliente	**AES-256 dichiarato** Google Cloud: cifratura AES-256 di default su tutti i layer. Workspace e Vertex AI: copertura dichiarata inclusi log e backup	**AES-256 dichiarato** Azure: cifratura AES-256 a riposo su tutti i servizi inclusi Log Analytics, Storage, backup. Customer-Managed Keys disponibili	**AES-256 dichiarato** Cifratura a riposo dichiarata; copertura esplicita su log/cache/debug non dettagliata quanto hyperscaler. Via AWS/Azure: standard del CSP applicato
8. Gestione delle chiavi crittografiche (CMK/BYOK, rotazione, revoca)				

Ambito di valutazione	OpenAI (ChatGPT Ent./API)	Google (Gemini / Vertex AI)	Microsoft (Azure OpenAI)	Anthropic (Claude Ent./API)
8.1 Customer-Managed Keys (CMK) / BYOK	EKM disponibile Enterprise Key Management (EKM): cliente porta le proprie chiavi per dati a riposo. Disponibile per Enterprise	CMEK disponibile Customer-Managed Encryption Keys (CMEK) su Vertex AI e Google Cloud. Integrazione con Cloud KMS o HSM esterno (BYOK)	CMK disponibile Azure Key Vault + Customer-Managed Keys per Azure OpenAI e tutti i servizi di storage correlati. Integrazione HSM dedicato possibile	Solo via CSP Anthropic API diretta: nessuna gestione chiavi client-side dichiarata. Via AWS Bedrock: AWS KMS + BYOK. Via Azure: Azure Key Vault. Dipende dal layer infrastrutturale
8.2 Rotazione, revoca e isolamento per tenant	Limitata documentazione EKM supporta rotazione; isolamento per tenant dichiarato logicamente. Dettagli operativi non completamente pubblici	Documentata Cloud KMS: rotazione automatica e manuale, revoca immediata. Isolamento per progetto/tenant garantito	Documentata Azure Key Vault: rotazione automatica, revoca, audit degli accessi alle chiavi. Isolamento per tenant Azure AD nativo	Solo via CSP Tutte le funzionalità KMS delegate al CSP sottostante (AWS/Azure). Nessuna feature KMS nativa Anthropic
9. Controllo accessi privilegiati del fornitore (chi accede ai dati)				
9.1 Dichiarazione e limitazione accessi interni	Parziale Politica zero-trust dichiarata. Accessi interni ai dati clienti non dettagliati pubblicamente; monitoraggio abuse da personale limitato	Access Transparency Google Cloud Access Transparency: log in tempo reale degli accessi Google al tenant. Access Approval: cliente approva o nega accessi. Disponibile per Vertex AI	Lockbox / Customer Lockbox Azure Customer Lockbox: richiesta esplicita e approvazione cliente per accesso Microsoft ai dati. Audit trail completo. Disponibile per Azure OpenAI	Non dettagliato Nessuna dichiarazione pubblica equivalente a Lockbox/Access Transparency. Processo di accesso privilegiato interno non documentato nel dettaglio
9.2 Accessi just-in-time e auditabili	Non dichiarato esplicitamente Zero trust come principio; JIT non dichiarato come feature disponibile al cliente	Documentato JIT access per operazioni interne dichiarato; Access Transparency audit log disponibile al cliente per verifica	Documentato Privileged Identity Management (PIM) Azure: JIT per accessi privilegiati. Audit log completo e consultabile dal cliente	Non dichiarato Non documentato pubblicamente. Affidarsi a garanzie del CSP se deployato su AWS/Azure
10. Gestione incidenti e notifica violazioni				

Ambito di valutazione	OpenAI (ChatGPT Ent./API)	Google (Gemini / Vertex AI)	Microsoft (Azure OpenAI)	Anthropic (Claude Ent./API)
10.1 Procedure incident response dichiarate	Documentate Security response team dedicato; DPA include obblighi incident response. Penetration est continui dichiarati	Documentate Google Cloud: procedure IR documentate; DPA include IR. FedRAMP richiede piani IR certificati	Documentate Microsoft Security Response Center (MSRC); DPA con IR; standard ISO 27035 per IR su Azure	Documentate Procedure IR nel DPA; security team dichiarato. Meno visibilità pubblica rispetto a hyperscaler su dettagli operativi
10.2 Notifica violazione dati (tempistiche, GDPR art. 33/34)	72h dichiarate nel DPA Notifica entro 72h all'autorità di controllo come da GDPR; supporto al cliente per notifica agli interessati	72h dichiarate nel DPA Notifica breach entro 72h; supporto DSAR e breach notification per clienti enterprise	72h dichiarate nel DPA Microsoft DPA: notifica entro 72h; Customer Lockbox audit consente tracciamento; MSRC referente per breach	72h dichiarate nel DPA DPA Anthropic: notifica breach entro 72h; procedure meno testate pubblicamente rispetto a provider con lunga storia enterprise
11. Minimizzazione dei dati (log e monitoring)				
11.1 Limitazione registrazione contenuto prompt nei log di sistema	Condizionato a ZDR Senza ZDR: input/output registrati per abuse monitoring (temporanei). ZDR elimina la persistenza. Non minimizzazione by-default	Richiede configurazione attiva Vertex AI ZDR + disabilitazione cache + opt-out abuse log: minimizzazione raggiungibile. Non attiva by-default. Workspace: no human review senza consenso	Dipende dalla modalità deployment Default: prompts non conservati dopo risposta (salvo abuse). EU DataZone: abuse monitoring in-region. Disabilitazione log abuse con approvazione. Non by-default per tutti i log di telemetria	API: più vicino a minimizzazione API 7 gg retention (da set. 2025); ZDR disponibile. Policy esplicita: nessun uso per training. Riduzione rilevante rispetto a periodo precedente
12. Gestione sub-fornitori e supply chain				
12.1 Elenco sub-processor dichiarato e aggiornato	Disponibile Lista sub-processor pubblicata e aggiornata nel DPA. Notifica preventiva 30 gg per modifiche	Disponibile Google Cloud: sub-processor list pubblica per GCP e Workspace. Notifica preventiva dei cambiamenti	Disponibile Microsoft Trust Center: lista sub-processor aggiornata per Azure. Online Services Sub-processor List consultabile	Disponibile DPA Anthropic: lista sub-processor dichiarata. Notifica preventiva cambiamenti. Principale sub-processor: AWS (infrastruttura)

Ambito di valutazione	OpenAI (ChatGPT Ent./API)	Google (Gemini / Vertex AI)	Microsoft (Azure OpenAI)	Anthropic (Claude Ent./API)
12.2 Localizzazione trattamenti sub-processor	**Parziale** Sub-processor prevalentemente USA. EU data residency limita ma non elimina il coinvolgimento di sub-processor extra-UE (SCC a copertura)	**Dettagliata** Google Cloud sub-processor list indica per ciascuno la localizzazione. Opzione EU-only restringe i sub-processor a entità UE/adeguate	**Dettagliata** Microsoft pubblica localizzazione sub-processor. EU Data Boundary restringe trattamenti a sub-processor operanti in UE/EEA per dati coperti	**Meno dettagliata** Lista disponibile ma dettaglio localizzazione meno granulare. AWS (US) principale sub-processor infrastrutturale
13. Isolamento tra tenant				
13.1 Isolamento logico/fisico tra clienti diversi	**Dichiarato (logico)** Architettura multi-tenant con isolamento logico; dati cliente non accessibili ad altri tenant. Dichiarazione esplicita nel DPA	**Dichiarato e certificato** Google Cloud: isolamento per progetto/organizzazione garantito. VPC Service Controls per perimetri di sicurezza. Certificato da audit SOC 2/ISO	**Dichiarato e certificato** Azure: isolamento per tenant Azure AD nativo. VNet, Network Security Groups, Private Endpoints. Certificato SOC 2/ISO 27001	**Dichiarato (logico)** Isolamento logico tra tenant dichiarato; copertura fisica dipende dal CSP sottostante. Garanzie meno granulari rispetto a hyperscaler

2.2. Note metodologiche e avvertenze

- **Perimetro temporale:** le informazioni si basano sulla documentazione pubblica disponibile a marzo 2026 (le politiche dei provider sono soggette a variazioni frequenti).
- **Qualificazione ACN:** allo stato della documentazione pubblica e del catalogo ACN, OpenAI e Anthropic non risultano dotati di qualificazione ACN diretta. Ai fini della PA, rileva quindi anche la qualificazione dell'infrastruttura cloud o del layer di erogazione attraverso cui il servizio viene fruito. La qualificazione del layer applicativo AI/SaaS richiede comunque verifica caso per caso nel catalogo ACN e nella documentazione del servizio.
- **(Zero Data Retention):** la modalità ZDR è la configurazione più restrittiva, ma non è sempre disponibile su tutti i piani; per i provider che la prevedono, essa è in genere subordinata a previa approvazione e a requisiti specifici. La sua adozione non esime comunque dalla verifica dell'intero perimetro tecnico del servizio, inclusi eventuali componenti accessori di sicurezza, filtraggio e monitoraggio.
- **Sovrapposizione GDPR/NIS2:** il quadro evidenzia deliberatamente le sovrapposizioni tra requisiti GDPR (artt. 25, 28, 32-34) e requisiti NIS2 (misure di sicurezza della catena di approvvigionamento, notifica incidenti, gestione del rischio). La distinzione è indiretta: un fornitore può soddisfare il GDPR ma non avere procedure NIS2-specifiche formalizzate.
- **Raccomandazione DPO:** per uso istituzionale della PA, si consiglia di prioritizzare provider con:
  a) qualificazione ACN del layer cloud di supporto;
  b) DPA sottoscritto e, ove necessario in relazione ai trasferimenti verso Paesi terzi, SCC o altro idoneo meccanismo di trasferimento;
  c) ZDR o retention minima configurata;
  d) BYOK/CMK;

e) Customer Lockbox o equivalente;
f) sub-processor list aggiornata con localizzazione UE verificata.

ALLEGATO 1

Amazon Web Services / Amazon Bedrock nel quadro comparativo NIS2/GDPR: ragioni dell'esclusione come colonna autonoma nel quadro sinottico e analisi di compliance

Il quadro sinottico assume come criterio di comparazione i provider del modello o del servizio di AI oggetto di analisi, non il soggetto che eroga l'infrastruttura cloud sottostante. In questa prospettiva, OpenAI, Google, Microsoft e Anthropic sono stati considerati quali soggetti che governano il modello o il servizio di AI esaminato.

Amazon Web Services, e in particolare la sua piattaforma Amazon Bedrock, non è stato incluso come colonna autonoma nella tabella principale non perché privo di rilievo, ma perché, nel presente elaborato, viene in considerazione principalmente quale layer infrastrutturale e di distribuzione attraverso cui modelli propri o di terzi possono essere resi disponibili. Amazon Bedrock, infatti, mette a disposizione in modo centralizzato più famiglie di modelli, inclusi modelli di terze parti e modelli Amazon.

L'inclusione di AWS è stata effettuata su specifica richiesta della Commissione ICT CRUI e ritenuta opportuna dal Gruppo ICT, in ragione del suo rilievo operativo quale layer di deployment di modelli di terzi e della sua incidenza sui profili di compliance infrastrutturale, contrattuale e di supply chain.

In tale prospettiva, la sua collocazione nella medesima tabella principale accanto ai quattro provider selezionati avrebbe rischiato di sovrapporre piani di analisi non perfettamente omogenei, generando confusione nella rappresentazione della catena di erogazione del servizio e dei relativi profili di compliance. La distinzione rileva sia sotto il profilo privacy, sia ai fini della due diligence NIS2 sulla supply chain, poiché il provider del modello e il layer infrastrutturale o distributivo possono assumere ruoli diversi, da valutare distintamente nella documentazione di compliance e nell'analisi della catena di approvvigionamento.

In tale contesto, la collocazione di AWS/Bedrock in allegato si giustifica ulteriormente in relazione a tre profili:

1. **AWS/Bedrock può costituire il layer di deployment di modelli di terzi, inclusi i modelli Anthropic Claude**

Ne deriva che, in concreti scenari di deployment istituzionale, la compliance del servizio non dipende soltanto dal provider del modello, ma anche dal layer infrastrutturale e di distribuzione attraverso cui il modello viene effettivamente fruito. Per questa ragione, l'analisi del solo provider del modello può non essere sufficiente a rappresentare integralmente il contesto operativo di utilizzo.

2. **AWS presenta un rilievo specifico nel contesto della qualificazione ACN e, più in generale, delle valutazioni di procurement pubblico per la PA italiana**

Tale rilievo assume particolare interesse anche nella misura in cui la fruizione istituzionale di alcuni dei modelli o servizi considerati nel quadro può avvenire, in concreto, attraverso infrastrutture o layer di distribuzione riconducibili ad AWS/Bedrock; sotto questo profilo, la qualificazione ACN del relativo layer infrastrutturale costituisce un elemento che merita autonoma considerazione. AWS ha infatti comunicato di aver ottenuto la qualificazione QC2 per 23 categorie di servizi e 228 prodotti rilevanti per la PA italiana.

3. **Il modello operativo di Bedrock presenta profili architetturali di particolare rilievo ai fini della compliance.**

La documentazione AWS evidenzia che Amazon Bedrock non memorizza né registra prompt e completions, non li utilizza per addestrare modelli AWS e non li distribuisce a terzi; evidenzia inoltre che i fornitori del modello non hanno accesso ai Model Deployment Accounts, ai log Bedrock né ai prompt e alle completions dei clienti. AWS dichiara, altresì, che, dopo la consegna del modello, viene eseguita una deep copy del software di inferenza e training del provider all'interno di account gestiti dal servizio. Si tratta di un assetto architetturale che assume rilievo non soltanto sul piano contrattuale, ma anche sotto i profili della segregazione, dell'accesso ai dati, del logging e del controllo della supply chain tecnologica, e che giustifica, per tale ragione, una valutazione distinta rispetto a quella del solo provider del modello.

A titolo esemplificativo, si riporta di seguito la valutazione di Bedrock sugli stessi assi del quadro sinottico.

Qualificazione ACN

QI2/QC2 diretta, valida dal 15 aprile 2024, per 228 prodotti e 23 categorie di servizi, inclusi workload critici PA.

ISO/IEC 27001 e certificazioni

Amazon Bedrock rientra nei programmi di compliance AWS che includono, tra gli altri, ISO/IEC 9001, 27001, 27017, 27018, 27701, 22301, 20000, CSA STAR e SOC; Bedrock AgentCore è inoltre indicato come HIPAA eligible e in percorso verso FedRAMP.

No training su dati cliente

Amazon Bedrock non usa prompt e completions per addestrare modelli AWS né li condivide con i fornitori del modello. Tale garanzia è supportata anche dall'assetto architetturale del servizio, che prevede account di deployment gestiti da Bedrock e separati dal model provider.

Residenza EU

Il DPA AWS si applica automaticamente ai clienti soggetti al GDPR e AWS documenta opzioni di trattamento dei dati e di deployment per regione. Per Amazon Bedrock, la disponibilità del servizio e dei modelli varia in funzione delle regioni AWS supportate; tra le regioni europee AWS figurano, tra le altre, Francoforte, Irlanda, Milano e Parigi, mentre Londra è regione europea ma non appartenente all'Unione europea.

GDPR / DPA

Il DPA AWS è incorporato direttamente nei Service Terms e si applica automaticamente a tutti i clienti che usano AWS per il trattamento di dati personali, senza necessità di sottoscrivere un addendum separato.

Logging e audit

Bedrock può essere integrato con i servizi AWS di logging e monitoraggio, inclusi AWS CloudTrail e Amazon CloudWatch, a supporto delle esigenze di audit, monitoraggio e integrazione con sistemi di sicurezza e governance.

Cifratura e gestione delle chiavi

I dati sono cifrati in transito e a riposo; è inoltre possibile creare, gestire e controllare le chiavi di cifratura mediante AWS KMS, incluse chiavi gestite dal cliente.

Accessi privilegiati

Come indicato al punto 3, l'assetto di Bedrock prevede la separazione tra gli account di deployment gestiti dal servizio e i model provider. AWS CloudTrail consente la registrazione delle operazioni API, mentre i controlli IAM e MFA contribuiscono alla gestione e tracciabilità degli accessi privilegiati.

Isolamento tenant

L'isolamento dei tenant si fonda sui meccanismi AWS di separazione a livello di account, rete, identità e gestione delle chiavi, nel quadro dei controlli di sicurezza e dei programmi di compliance AWS applicabili al servizio.