Quadro sinottico NIS2 / GDPR / AI Act

Compliance dei provider AI per il sistema universitario

Gruppo ICT CRUI

Revisione giugno 2026 | Include sezione AI Act (Reg. UE 2024/1689)

OpenAI | **Google** | **Microsoft** | **Anthropic**

Perché questo documento

Gruppo ICT CRUI · Revisione giugno 2026

Un quadro normativo in evoluzione rapida

NIS2, GDPR e AI Act si applicano cumulativamente agli stessi contratti. Gli atenei devono valutare i provider su tre piani normativi contemporaneamente, con scadenze diverse e obblighi asimmetrici tra provider e deployer.

Frammentazione delle informazioni

Le dichiarazioni dei provider sono disperse tra DPA, Trust Center, pagine security e documentazione API. Il Gruppo ICT ha centralizzato e verificato oltre 40 fonti primarie, distinguendo ciò che è verificato da ciò che è dichiarato.

Specificità del sistema universitario

Gli atenei operano come PA e come deployer AI: soggetti a NIS2, al GDPR per i dati di studenti e personale, e agli obblighi AI Act sul deployer, inclusa l'AI literacy già applicabile dal 2 febbraio 2025.

Perimetro e struttura della valutazione

Gruppo ICT CRUI · Revisione giugno 2026

4 PROVIDER ANALIZZATI

- **OpenAI** — ChatGPT Ent./API
- **Google** — Gemini / Vertex AI
- **Microsoft** — Azure OpenAI
- **Anthropic** — Claude Ent./API

14 AMBITI DI VALUTAZIONE

1. Qualificazione ACN e certificazioni
2. Conformità GDPR / DPA, diritti, base giuridica
3. Divieto uso dati per training e debug
4. Residenza dei dati in UE
5. Logging e configurabilità
6. Politiche di retention
7. Cifratura in transito e a riposo
8. Rotazione e isolamento chiavi
9. Accessi privilegiati del fornitore
10. Gestione incidenti e notifica violazioni
11. Minimizzazione dei dati
12. Sub-fornitori e supply chain
13. Isolamento tra tenant
14. AI Act / GPAI, rischio sistemico, Code of Practice

Il metodo: trasparenza epistemica

Gruppo ICT CRUI · Revisione giugno 2026

Ogni affermazione nel documento è etichettata con il suo livello di certezza. Il lettore sa sempre se un'informazione è stata verificata su fonte primaria, dichiarata dal fornitore, o ancora da verificare.

✓ Verificato

Fonte primaria letta direttamente: sito ufficiale del provider, Trust Center, documentazione API, atto di autorità di controllo. URL e data di lettura citati in modo esplicito.

40+ fonti primarie lette

📋 Dichiarato dal fornitore

Affermazione che proviene da DPA, Product Terms o pagine security del fornitore. Non verificata da terzi indipendenti. È la norma per questo tipo di valutazione: la PA si fida della dichiarazione contrattuale.

Standard di settore

📋 Certificazione: report richiedibile

Il fornitore dichiara di aver ottenuto una certificazione. Il report è redatto da ente terzo accreditato ma non è pubblico: va richiesto tramite Trust Center, spesso previo NDA.

SOC 2, ISO 27001, ISO 42001…

⚠ Da verificare

Fonte non letta direttamente in questa revisione. Le voci residue riguardano clausole contrattuali accessibili solo con un contratto attivo, o pagine che richiedono autenticazione.

Ridotto al minimo

AI come strumento, competenza come metodo

Gruppo ICT CRUI · Revisione giugno 2026

Contributo dei sistemi AI

→ Recupero sistematico di fonti da oltre 40 URL ufficiali

→ Confronto incrociato tra versioni successive dei documenti dei provider

→ Strutturazione della tabella su 14 ambiti e 4 provider

→ Identificazione delle discontinuità tra dichiarazioni e documentazione

→ Drafting delle note metodologiche e delle correzioni critiche

→ Generazione e validazione del documento Word finale

⟷

validato e corretto dal Gruppo ICT

Competenza del Gruppo ICT

→ Definizione del perimetro normativo e degli ambiti rilevanti per la PA

→ Verifica diretta su fonte primaria di ogni affermazione critica

→ Correzione di errori fattuali generati da fonti secondarie (es. pinning EU Anthropic)

→ Identificazione e contestualizzazione dei bias nelle dichiarazioni dei provider

→ Valutazione della rilevanza giuridica delle singole clausole per il contesto universitario

→ Decisione finale su ogni marcatore epistemico e ogni nota metodologica

Correzioni critiche: quando la verifica fa la differenza

Gruppo ICT CRUI · Revisione giugno 2026

Alcune informazioni circolate in fonti secondarie sono risultate errate o fuorvianti. La verifica su fonte primaria le ha corrette.

Anthropic

❌ API diretta con pinning regionale EU disponibile

✓ Il parametro inference_geo non supporta 'eu'. L'unica opzione per residenza EU è AWS Bedrock EU-region o Vertex AI EU.

Impatto: Un ateneo che avesse basato la propria DPIA su questa informazione avrebbe valutato erroneamente la conformità GDPR.

Microsoft Azure OpenAI

❌ Customer Lockbox disponibile per Azure OpenAI

✓ Azure OpenAI è escluso dall'applicazione della policy Customer Lockbox per default, salvo dichiarazione esplicita.

Impatto: Rilevante per la valutazione degli accessi privilegiati del fornitore ai dati del cliente.

Google (cella 2.3)

❌ Multa CNIL a Google come indicatore di rischio per i servizi AI enterprise

✓ La deliberazione SAN-2025-004 (€325M) riguarda esclusivamente Gmail consumer e cookie. Non impatta Workspace o Vertex AI.

Impatto: Contestualizzazione errata avrebbe penalizzato ingiustamente Google nei confronti enterprise.

Lettura d'insieme: punti di forza e di attenzione

Gruppo ICT CRUI · Revisione giugno 2026

Selezione degli ambiti più critici per la PA. Il quadro completo è nel documento.

Ambito	OpenAI	Google	Microsoft	Anthropic
Qualificazione ACN	Tramite Azure (verifica scheda)	Livello 2 (schede specifiche)	Tramite PSN (schede specifiche)	Non qualificata
Data residency UE	Disponibile (Enterprise/API)	Disponibile (Vertex AI / Workspace)	Disponibile con EU DataZone ⚠ Flex Routing	Solo via AWS Bedrock / Vertex AI EU
Divieto training (enterprise)	Garantita	Garantita (Vertex AI / Workspace)	Garantita	Garantita per API/commerciale
Accessi privilegiati fornitore	Parziale — JIT non documentato	Access Transparency disponibile ✓	⚠ Lockbox non copre Azure OpenAI	Non dichiarato
AI Act — GPAI Code of Practice	Firmatario (tutti e 3 i capitoli)	Firmatario (tutti e 3 i capitoli)	Firmatario (tutti e 3 i capitoli)	Firmatario (tutti e 3 i capitoli)

Conforme / Disponibile

Parziale / Da valutare

Non disponibile / Non dichiarato

AI Act: la dimensione che cambia il perimetro

Gruppo ICT CRUI · Revisione giugno 2026

Obblighi del PROVIDER (GPAI)

→ Documentazione tecnica (art. 53): già applicabile

→ Sommario dati di training: già applicabile

→ Cooperazione con l'AI Office

→ Valutazione rischio sistemico (se >10^{25} FLOP)

→ Tutti e 4 i provider hanno firmato il GPAI Code of Practice

Obblighi dell'ATENEO (deployer)

→ AI literacy del personale: GIÀ APPLICABILE dal 2 feb 2025

→ Verifica pratiche vietate: GIÀ APPLICABILE

→ DPIA + impatto diritti fondamentali (sistemi ad alto rischio)

→ Registrazione sistemi ad alto rischio nel database UE

→ LLM generici NON sono ad alto rischio di per sé (dipende dall'uso)

Come usare il documento

Gruppo ICT CRUI · Revisione giugno 2026

01 Supporto alla negoziazione contrattuale

Il documento identifica le clausole che richiedono verifica prima della firma (DPA, diritti di audit, sub-processor list). Le voci ⚠ indicano dove richiedere documentazione integrativa al fornitore tramite Trust Center o NDA.

02 Input per la DPIA

La sezione sulla residenza dei dati, sul divieto di training e sugli accessi privilegiati fornisce elementi fattuali per la valutazione d'impatto sulla protezione dei dati. I marcatori epistemici indicano quali elementi necessitano di ulteriore verifica.

03 Checklist per il responsabile IT

Il quadro segnala le impostazioni critiche da verificare prima del deployment: Flex Routing Microsoft, endpoint EU su Vertex AI, configurazione EKM su OpenAI, inference_geo su API Anthropic.

04 Riferimento per l'adempimento AI Act

La sezione 14 chiarisce gli obblighi già applicabili per l'ateneo come deployer (AI literacy dal 2 febbraio 2025) e quelli in arrivo (agosto 2026), con la distinzione dal regime applicabile ai provider.

Un lavoro condiviso per il sistema universitario italiano

14 ambiti di valutazione · 4 provider · 40+ fonti primarie verificate

NIS2 · GDPR · AI Act in un unico documento integrato

Disponibile agli enti aderenti ai contratti CRUI

Gruppo ICT CRUI

Revisione giugno 2026