

ALLEGATO INFORMATIVO

EU AI Act, IA Cloud e IA On Premise

Overview informativa per aziende su governance, dati, rischio e scelte
architettoniche

Versione: giugno 2026

Documento informativo per aziende, utilizzabile come base di presentazione e
confronto con la direzione aziendale.

Perché questo documento

L'adozione dell'intelligenza artificiale non riguarda solo la scelta dello strumento più potente. Riguarda anche dove vengono trattati i dati, chi controlla gli accessi, quali output vengono prodotti e quale impatto possono avere su clienti, lavoratori, candidati o soggetti terzi.

Questo documento offre una panoramica sintetica su EU AI Act, uso aziendale dell'IA, cloud, private cloud e IA on premise. L'obiettivo è aiutare il cliente a capire quando una soluzione standard può bastare e quando è invece opportuno valutare architetture più controllate.

EU AI Act in sintesi

L'EU AI Act, Regolamento UE 2024/1689, è il quadro normativo europeo dedicato all'intelligenza artificiale. Il regolamento adotta un approccio basato sul rischio: gli obblighi cambiano in base al tipo di sistema, alla finalità d'uso, ai dati trattati e all'impatto sulle persone.

Livello di rischio	Descrizione pratica
Rischio inaccettabile	Pratiche vietate perché incompatibili con diritti fondamentali o valori europei.
Alto rischio	Sistemi usati in ambiti delicati, come HR, sanità, istruzione, credito, servizi essenziali o processi con impatto sulle persone.
Rischio di trasparenza	Chatbot, assistenti virtuali, deepfake, immagini, audio, video o contenuti sintetici che richiedono informazione chiara all'utente.
Rischio minimo o limitato	Molti usi ordinari di supporto, come bozze, traduzioni, sintesi, brainstorming e supporto operativo a basso impatto.

Perché riguarda anche chi usa IA, non solo chi la sviluppa

Molte aziende pensano che l'AI Act riguardi solo i produttori di modelli o le grandi piattaforme tecnologiche. In realtà il regolamento interessa anche i deployer, cioè le organizzazioni che usano sistemi IA in modo professionale.

Un'azienda che usa chatbot, strumenti generativi, software HR, CRM con funzioni IA, sistemi di analisi automatizzata, automazioni documentali o agenti IA deve comunque gestire aspetti come formazione, regole interne, controllo umano, trasparenza e documentazione.

Cloud, cloud business, private cloud e on premise

Architettura	Quando può essere adeguata	Attenzioni principali
Cloud pubblico controllato	Bozze, testi generici, brainstorming, traduzioni e contenuti non riservati.	Policy interna, divieto dati sensibili, controllo output.
Cloud business / enterprise	Uso aziendale più strutturato con account, ruoli, gestione utenti e condizioni contrattuali più solide.	DPA, retention, training sui dati, data residency, log, accessi.
Private cloud	Dati riservati o processi importanti, senza voler gestire infrastruttura interna.	Ambiente dedicato, sicurezza, contratti, auditabilità.
On premise	Documenti riservati, database interni, agenti aziendali, RAG su knowledge base, dati che non devono uscire dal perimetro aziendale.	Hardware, manutenzione, sicurezza, backup, accessi, log, monitoraggio.
Ambiente isolato	Contesti molto sensibili: sanità, legale, finanza, industria, dati strategici o vincoli contrattuali forti.	Costi e complessità maggiori; necessità di governance rigorosa.

Quando entra in gioco l'IA on premise

L'on premise non è un obbligo automatico dell'AI Act. Entra in gioco come possibile misura tecnica e organizzativa quando il tipo di dati o di processo rende preferibile mantenere maggiore controllo interno.

- Documenti aziendali riservati o coperti da accordi di riservatezza.
- Contratti clienti e fornitori.
- Dati personali, HR, CV, valutazioni candidati o dipendenti.
- Dati sanitari, finanziari, contabili o legali.
- Database clienti, procedure interne, manuali tecnici o know-how proprietario.
- Agenti IA collegati a sistemi interni o knowledge base aziendali.
- Vincoli contrattuali o regolatori che limitano il trasferimento dei dati.
- Necessità di log, tracciabilità, accessi granulari e controllo più forte.

Nota operativa: la domanda corretta non è 'serve per forza l'on premise?', ma 'quale architettura è proporzionata ai dati, ai processi e al rischio dell'azienda?'.

On premise non significa automaticamente conforme

Installare un modello locale o un sistema IA presso il cliente non rende automaticamente l'azienda conforme. Riduce alcuni rischi di esposizione dei dati, ma non elimina gli obblighi di governance.

- Serve comunque un registro IA.
- Serve classificare i casi d'uso.
- Serve formare il personale.
- Serve controllare accessi e autorizzazioni.
- Serve monitorare output, errori e incidenti.
- Serve definire responsabilità e supervisione umana.
- Serve valutare privacy, sicurezza e dati personali.
- Nei casi sensibili serve coinvolgere DPO, privacy o legale.

Matrice rapida di decisione

Scenario	Soluzione da valutare	Nota
Bozze email generiche	Cloud controllato	Policy e controllo output.
Marketing non sensibile	Cloud controllato o business	Attenzione a contenuti e dati cliente.
Documenti interni riservati	Private cloud o on premise	Valutare rischi di data leakage.
Contratti clienti	Private cloud o on premise	Coinvolgere privacy/legal se necessario.
Dati HR o CV	Private cloud/on premise con forte governance	Possibile area ad alto rischio.
Dati sanitari	On premise o ambiente altamente controllato	Coinvolgimento DPO/legal raccomandato.
Chatbot verso clienti	Cloud business, private cloud o on premise	Serve trasparenza verso l'utente.
Knowledge base aziendale	Private cloud o on premise	Scenario tipico per sistemi RAG controllati.

Roadmap consigliata per decidere l'architettura

- Mappare gli strumenti IA già utilizzati e i reparti coinvolti.
- Analizzare dati caricati, finalità, output e impatti sui processi aziendali.
- Classificare ogni caso d'uso in base al rischio.
- Valutare privacy, sicurezza, fornitori, retention, log e accessi.
- Decidere se usare cloud controllato, cloud business, private cloud, on premise o ambiente isolato.
- Definire policy interna, autorizzazioni e responsabilità.
- Formare il personale e conservare evidenza della formazione.
- Monitorare periodicamente nuovi strumenti, incidenti, output e cambiamenti normativi.

Vantaggi e limiti dell'on premise

Vantaggi	Limiti
Maggiore controllo sui dati e sui documenti interni.	Costi hardware e infrastrutturali più alti.
Riduzione dell'esposizione verso piattaforme esterne.	Necessità di manutenzione e competenze tecniche.
Accessi, log e ruoli più governabili.	Prestazioni talvolta inferiori rispetto ai migliori modelli cloud.
Possibilità di integrare knowledge base e sistemi interni.	Responsabilità diretta su sicurezza, backup e aggiornamenti.
Maggiore coerenza con policy e vincoli aziendali.	Non elimina gli obblighi di governance e controllo umano.

Domande da porsi prima di scegliere

- Quali strumenti IA vengono già usati e da chi?
- Quali dati vengono inseriti nei sistemi IA?
- Sono presenti dati personali, sensibili o riservati?
- Gli output influenzano decisioni su persone?
- Il fornitore conserva i dati o li usa per training?
- Esistono vincoli contrattuali sulla riservatezza?
- Serve tracciare chi ha interrogato il sistema e con quali documenti?
- Serve interrogare documenti o database aziendali interni?
- L'azienda ha risorse tecniche per gestire un sistema on premise?
- Quali aree richiedono coinvolgimento di DPO, privacy o legale?

Conclusione

La scelta tra IA cloud, privata o on premise deve essere proporzionata al rischio. Per usi semplici e non sensibili, il cloud può essere adeguato se regolato correttamente. Per dati riservati, processi critici o integrazioni con sistemi interni, può essere opportuno valutare soluzioni private o on premise.

Il punto non è scegliere la tecnologia più complessa, ma quella più coerente con dati, responsabilità e obiettivi dell'azienda. La governance resta indispensabile in ogni scenario.

Limiti del documento

Avvertenza: il presente documento ha natura informativa, organizzativa e consulenziale. Non costituisce parere legale, certificazione di conformità, valutazione privacy formale o sostituzione delle attività spettanti a DPO, consulenti legali, organismi notificati o autorità competenti. Nei casi che coinvolgono dati personali, sistemi ad alto rischio, processi decisionali automatizzati o settori regolati, è opportuno prevedere il coinvolgimento di figure specialistiche.

Fonti istituzionali consultate

Le fonti seguenti sono state utilizzate come riferimento generale. Il cliente dovrà comunque verificare eventuali aggiornamenti normativi e applicativi con consulenti legali, privacy o autorità competenti.

- Commissione europea - AI Act, quadro regolatorio e timeline:
<https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>
- Commissione europea - AI literacy, domande e risposte:
<https://digital-strategy.ec.europa.eu/en/faqs/ai-literacy-questions-answers>
- Commissione europea - AI talent, skills and literacy:
<https://digital-strategy.ec.europa.eu/en/policies/ai-talent-skills-and-literacy>
- AI Act Service Desk - Articolo 26, obblighi dei deployer di sistemi ad alto rischio:
<https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-26>
- Malta Digital Innovation Authority - Artificial Intelligence: <https://mdia.gov.mt/services/artificial-intelligence/>