

**RISORSE**

AI in azienda: cosa chiede la legge e come proteggere i **dati**

Due domande che arrivano in ogni corso: "cosa ci obbliga a fare l'AI Act?" e "possiamo dare all'AI i nostri documenti?". Le risposte, in poche pagine, per qualsiasi strumento: ChatGPT, Claude, Gemini, Grok, Copilot.

Scritto con l'aiuto dell'AI, rivisto da Mauro Milesi · aggiornato al 23 ottobre 2026

A CHI SERVE

Titolari, responsabili e chiunque in ufficio usi l'AI con documenti di lavoro

LE DUE PARTI

1. AI Act: cosa chiede la legge · 2. Sicurezza dei dati: cosa tutela l'azienda

COME SI LEGGE

Ogni fonte citata è un link alla pagina ufficiale: norme e condizioni dei fornitori cambiano, verificale prima di decidere

Due norme diverse, da non confondere

L'[AI Act](#) regola come si costruiscono e si usano i sistemi di intelligenza artificiale. Il [GDPR](#) regola come si trattano i dati personali. Si applicano insieme: un'azienda può essere in regola con l'AI Act e violare comunque la privacy, per esempio se un dipendente carica i dati dei clienti sul suo account AI personale.

E il GDPR vieta l'AI americana?

No. Trasferire dati a un fornitore negli Stati Uniti è lecito con le garanzie del GDPR: l'adesione al Data Privacy Framework UE-USA, [riconosciuto dalla Commissione nel 2023](#), oppure le clausole contrattuali standard, più un accordo sul trattamento dei dati. Il rischio nasce altrove: account personali usati per dati di terzi, contratto assente, dati sanitari senza valutazione d'impatto, informativa che non cita l'AI. Due rischi residui: il [ricorso contro il Data Privacy Framework](#) è ancora pendente, e i fornitori americani sono soggetti al [CLOUD Act](#).



Parte 1. AI Act: cosa chiede la legge

L'AI Act è il regolamento europeo sull'intelligenza artificiale. Non riguarda solo chi sviluppa l'AI: si applica anche a chi la **usa** nella propria attività. Basta una persona che usa uno strumento AI per lavoro. Gli obblighi dipendono da quanto è rischioso l'uso: per gli usi d'ufficio più comuni sono pochi e chiari. Nel 2026 il [regolamento \(UE\) 2026/1744](#), l'Omnibus digitale, ha rinviato le regole sull'alto rischio, non il resto.

I livelli di rischio, con esempi d'ufficio

Livello	Esempi	Cosa comporta
Vietato	Riconoscere le emozioni dei dipendenti sul lavoro, punteggio sociale	Non si può fare, salvo motivi medici o di sicurezza
Alto rischio	Filtrare CV, valutare candidati, misurare le prestazioni dei lavoratori	Sorveglianza umana, informazione ai lavoratori, controlli
Trasparenza	Immagini, audio e video realistici generati con l'AI e pubblicati	Dichiarare che sono generati. Per i testi su temi di interesse pubblico, solo se nessuno li ha rivisti
Minimo	Riassumere documenti, scrivere bozze di email, analizzare un file Excel	La formazione del personale che li usa

Cosa fare in pratica

- Fare l'elenco degli strumenti AI usati in azienda, anche quelli usati di propria iniziativa.
- Formare il personale che li usa, e tenerne traccia: programma, date, partecipanti.
- Dichiarare immagini, audio e video realistici generati con l'AI quando si pubblicano.
- Informare i lavoratori se l'AI entra nella gestione del personale, e lasciare a una persona la decisione finale.

In sintesi: per legge, la formazione non è facoltativa

Chi usa l'AI deve adottare misure per formare il personale che la usa: cosa fa bene, dove sbaglia, quali rischi comporta. L'Omnibus ha precisato che non serve garantire un livello preciso, servono misure adatte alle persone e al contesto. Vale già per tutte le aziende, piccole comprese, e una formazione documentata è il modo più semplice per dimostrarlo.



Il calendario

Dal	Cosa si applica
2 febbraio 2025	Divieti e obbligo di formare il personale che usa l'AI
10 ottobre 2025	Legge italiana: il datore di lavoro informa i lavoratori quando usa l'AI, il professionista informa i clienti (legge 132/2025 , art. 11 e 13)
2 agosto 2026	Trasparenza; da qui l'AI Act si applica in generale, vigilanza compresa
23 ottobre 2026	Italia: AgID e ACN con poteri di controllo e sanzione. Nelle decisioni sul personale la decisione finale resta a una persona: un licenziamento deciso solo da un sistema automatico è nullo (d.lgs. 179/2026 , art. 41)
2 dicembre 2026	Marcatura dei contenuti generati; nuovi divieti sulle immagini intime non consensuali
2 dicembre 2027	Alto rischio, Allegato III: CV, candidati, valutazione dei dipendenti
2 agosto 2028	Alto rischio, Allegato I: AI nei prodotti già regolati, come dispositivi medici o giocattoli

Parte 2. Sicurezza dei dati: cosa tutela l'azienda

Regola base: l'AI non si porta via l'archivio, ma **tutto ciò che legge per risponderti passa dal fornitore**. Conta quale versione dello strumento usi, con quale contratto e chi può vedere cosa.

Account personale o aziendale: la differenza che conta davvero

	Account personale (gratuito o abbonamento individuale)	Account aziendale (piani business, Enterprise, API)
Contratto	Tra il fornitore e la persona, non con l'azienda	Con l'azienda, con accordo sul trattamento dei dati (DPA)
Addestramento	Può essere usato, a seconda del fornitore e delle impostazioni: va controllato e disattivato	Non attivo per impostazione predefinita

Modelli e strumenti: non sono la stessa cosa

Il **modello** è il motore: GPT di OpenAI, Claude di Anthropic, Gemini di Google, Grok di xAI. Lo **strumento** è l'app che lo usa: Copilot, per esempio, usa modelli OpenAI, Anthropic e modelli propri di Microsoft. Per i dati conta il contratto dello strumento.



Strumento aziendale	Cosa sapere
Microsoft 365 Copilot	Lavora sotto i contratti Microsoft già firmati; prompt e documenti non addestrano i modelli. Dati nel perimetro UE, con due eccezioni: ricerca web e modelli Anthropic. Vede ciò che vede l'utente: prima si controllano i permessi. Fonte , eccezioni
ChatGPT (OpenAI)	Business, Enterprise e API: niente addestramento per impostazione predefinita, DPA disponibile. Dati conservati in Europa per le nuove aree di lavoro Enterprise ed Edu e per i progetti API idonei. Fonte , dati in Europa
Claude (Anthropic)	Piani commerciali: niente addestramento per impostazione predefinita, DPA nei termini. Comprando da Anthropic oggi non c'è una regione UE; in Europa si passa da Amazon Bedrock con il profilo europeo. Fonte , regioni , Bedrock
Gemini (Google Workspace)	Con un'edizione Workspace idonea, niente addestramento senza permesso. Regione UE selezionabile: archiviazione in UE con le regioni dei dati, anche l'elaborazione solo con le regioni "Enterprise" o "Assured Controls". Fonte , regioni
Grok (xAI)	Niente addestramento sui dati business, salvo accordo; DPA nei termini enterprise. Nessuna regione UE documentata: per l'API esiste solo un endpoint USA. Fonte , regioni

Altre strade: Europa, Cina, in casa

Fornitori europei, per esempio Mistral: dati nell'UE per impostazione predefinita, con alcune funzioni che li trasferiscono temporaneamente fuori UE con clausole standard; il piano Enterprise è escluso dall'addestramento ([dati](#), [addestramento](#)). **App cinesi**, per esempio DeepSeek: dati conservati in Cina; il 30 gennaio 2025 il Garante privacy ne ha limitato il trattamento in Italia ([provvedimento](#)). **Modelli in locale** (Llama, Mistral, Qwen, per esempio con [Ollama](#)): i dati non escono, ma servono hardware e competenze.

Il rischio vero di oggi: l'AI usata di nascosto

Il caso più comune è il collega che carica un file di lavoro sul suo account personale perché l'azienda non gli ha dato un'alternativa. Vietare l'AI non funziona: si continua a usarla senza dirlo. Servono uno strumento aziendale e una regola scritta su cosa si può caricare e dove.



Il semaforo dei dati: cosa si può caricare e dove

Livello	Esempi	Dove può andare
 Verde , pubblico	Testi del sito, schede prodotto già pubblicate, email generiche	Qualsiasi strumento
 Giallo , interno	Procedure, verbali, listini, offerte commerciali	Solo account aziendali con accordo sul trattamento dei dati
 Arancione , riservato	Bilanci non pubblicati, dati dei clienti, contratti, progetti in sviluppo	Account aziendali configurati, permessi verificati, meglio con dati in Europa
 Rosso , critico	Dati sanitari, buste paga, segreti industriali	Prima la valutazione d'impatto; poi anonimizzazione o un modello in locale

Il trucco più semplice: **anonimizzare prima di caricare**. "Cliente A, fatturato X" al posto di nomi e cifre reali: all'AI serve la struttura dei dati, quasi mai l'identità delle persone.

Supporto operativo su AI Act e GDPR applicato agli strumenti digitali. Non sostituisce la consulenza di un legale o di un DPO per gli aspetti giuridici formali.

Vuoi portarlo sui vostri strumenti e documenti?

Legge e sicurezza portano allo stesso punto: contratti e impostazioni proteggono fino a un certo punto, poi conta quello che le persone fanno ogni giorno davanti allo schermo. Organizzo percorsi su AI Act e uso sicuro dell'AI per PMI ed enti, in aula, online o in azienda. Scrivi a info@milesimauro.it o chiama il 371 746 1811.

PRENOTA UNA VIDEOCHIAMATA →