

AI Act 2026

5 step concreti

per una PMI italiana

(senza panico, senza consulenza legale costosa nelle prime settimane)

A chi serve questa guida

Imprenditori, CEO, IT manager e operations di PMI italiane (5–200 dipendenti) che usano già ChatGPT, automazioni, chatbot o sistemi predittivi — e si stanno chiedendo se stanno operando nel rispetto dell'AI Act, che è già in vigore.

Cosa NON è questa guida

Non è consulenza legale. È un percorso operativo: i 5 passi che facciamo con i clienti *prima* di sentire un legale specializzato. Senza questa base, qualunque consulenza diventa generica.

Indice

1. Perché l'AI Act riguarda anche te (anche se non vendi AI)
2. Step 1 — Mappa gli strumenti AI già in uso
3. Step 2 — Classifica il livello di rischio
4. Step 3 — Definisci una policy interna chiara
5. Step 4 — Documenta chi decide e con quali dati
6. Step 5 — Forma i referenti interni
7. Checklist finale per fare l'audit in azienda in un'ora
8. Prossimi passi

1. Perché l'AI Act riguarda anche te

L'AI Act europeo è in vigore dal 2024 e le sue scadenze si applicano per fasi tra il 2025 e il 2027. Non riguarda solo chi *produce* sistemi AI, ma anche chi li **integra nei propri processi**. E questo include praticamente ogni azienda italiana che oggi usa ChatGPT, sistemi predittivi, chatbot, generative tools per il marketing, o AI in produzione.

Il rischio non è solo la sanzione (che può arrivare al 7% del fatturato globale per le violazioni più gravi). Il rischio reale per una PMI è duplice:

1. Esposizione legale silenziosa. Strumenti AI usati senza policy possono violare GDPR, riservatezza commerciale e specifici divieti dell'AI Act senza che nessuno in azienda se ne accorga.

2. Perdita di valore in fase di audit/due diligence. Sempre più committenti chiedono ai fornitori di dichiarare come usano l'AI. Senza una mappa documentata, l'azienda perde contratti.

La buona notizia: nei prossimi 5 step ti diamo l'ossatura per arrivare ad avere **una governance proporzionata alla tua dimensione**, in 3–4 settimane di lavoro interno.

2. Step 1 — Mappa gli strumenti AI già in USO

Cosa fare

Mezzogiornata di interviste rapide con i responsabili di ogni reparto. Una domanda chiave: **“Quali strumenti che generano testo, immagini, previsioni o decisioni automatiche usate, anche solo saltuariamente?”**

Cosa mappare per ogni strumento

- Nome dello strumento (ChatGPT, Copilot, Claude, Midjourney, Notion AI, sistemi predittivi del gestionale, chatbot del sito, ecc.)
- Reparto e persona che lo usa
- Tipo di dato che viene inserito (commerciale, produttivo, anagrafiche clienti, fornitori, candidati)
- Frequenza (quotidiana, settimanale, sporadica)
- Se serve a prendere decisioni operative o solo a velocizzare task

Output

Un foglio di lavoro semplice (Excel o Google Sheet) con una riga per strumento. Nella nostra esperienza, una PMI da 30 persone scopre **tipicamente 8–15 strumenti AI attivi**, di cui solo 2–3 noti al management.

Tempo stimato

2–3 giorni di lavoro distribuito.

3. Step 2 — Classifica il livello di rischio

L'AI Act definisce 4 categorie di rischio per i sistemi AI. Per ciascuno strumento mappato nello Step 1, assegna una categoria.

Categoria	Esempi tipici in PMI	Cosa serve fare
Rischio inaccettabile (vietato)	Sistemi di social scoring, manipolazione subliminale	Dismettere immediatamente sul lavoro
Alto rischio	AI che screen-a candidati, valuta credito, prende decisioni produttive	Implementare controlli e supervisione umana, audit periodici
Rischio limitato	Chatbot customer-facing, generazione contenuti	Implementare misure di mitigazione, il cliente deve sapere che parla con un'AI
Rischio minimo	ChatGPT per email interne, Copilot per produttività	Implementare misure di mitigazione

Tempo stimato

1 giornata.

4. Step 3 — Definisci una policy interna chiara

La policy AI di una PMI non deve essere lunga 60 pagine. Deve essere lunga **4–6 pagine**, scritta in italiano comprensibile, approvata dal CEO in una riunione, e affissa (o condivisa) ovunque sia visibile.

Sezioni minime

- **Scopo:** perché abbiamo una policy AI (1 paragrafo)
- **Strumenti approvati:** lista chiara di cosa il team può usare (con versione, se rilevante)
- **Dati che NON possono uscire:** dati personali clienti, dati commerciali sensibili, prezzi, listini fornitori, formule, design protetti
- **Chi decide:** per ogni reparto, chi firma l'introduzione di un nuovo strumento AI
- **Decisioni automatizzate:** lista chiara delle decisioni che devono restare umane (assunzioni, valutazioni, accettazione ordini sopra X)
- **Procedura di emergenza:** chi chiamare se sospetti un uso scorretto o un data leak

Suggerimento operativo: non partire da template di multinazionali. Scrivila come scriveresti un'istruzione operativa per un nuovo assunto.

Tempo stimato

1 settimana, con 2–3 cicli di revisione.

5. Step 4 — Documenta chi decide e con quali dati

Per gli strumenti di **alto rischio** e **rischio limitato** emersi nello Step 2, serve una scheda di documentazione. Una sola pagina per strumento. Questa è la differenza tra essere preparati a un audit e prendere una sanzione.

Scheda strumento — campi minimi

- Nome strumento, fornitore, versione
- Categoria di rischio (Step 2)
- Tipo di decisioni/output che produce
- Dataset di input: che dati vengono passati, di chi sono
- Validazione umana: chi controlla l'output prima dell'azione
- Trasparenza verso l'utente finale (se applicabile)
- Data di valutazione e data prossima revisione (annuale)

Tempo stimato

1 settimana per documentare 5–10 strumenti.

6. Step 5 — Forma i referenti interni

Una governance senza persone formate è un PDF morto in un drive. Identifica un **referente AI per reparto** (3–5 persone in totale per una PMI media). Non devi formarli per *usare* l'AI, ma per **governarla**: applicare la policy, validare nuove richieste, segnalare zone grigie.

Cosa coprire nella formazione (4 ore in totale)

- 1 ora — Cos'è l'AI Act, perché ci riguarda, le 4 categorie di rischio
- 1 ora — Come leggere la policy aziendale, casi pratici reparto per reparto
- 1 ora — Come compilare la scheda strumento (Step 4)
- 1 ora — Come reagire a richieste nuove (es. un fornitore propone un tool AI)

Tempo stimato

2 mezze giornate distribuite su 2 settimane.

7. Checklist finale

Per fare l'audit AI in azienda in un'ora

- 1. Esiste una lista degli strumenti AI usati in azienda?
- 2. Ognuno di questi strumenti ha una categoria di rischio assegnata?
- 3. Esiste una policy AI scritta, approvata dal CEO?
- 4. I dati sensibili (clienti, prezzi, formule) sono chiaramente fuori da quello che può finire in un modello AI esterno?
- 5. Le decisioni automatizzate ad alto rischio hanno sempre una validazione umana?
- 6. C'è almeno un referente AI formato per ogni reparto principale?
- 7. C'è una scheda di documentazione compilata per i sistemi ad alto rischio?
- 8. È stata fissata una data di revisione annuale del sistema di governance?

Se hai meno di 5 sì su 8: hai un'esposizione significativa. È il momento di partire.

Se hai 5–7 sì: sei in mezzo. Manca la documentazione o la formazione, in genere.

Se hai 8 sì: complimenti, sei sopra la media.

8. Prossimi passi

Questi 5 step coprono il **fondamento operativo**. Sono ciò che fai prima di chiamare un legale. Senza questa base, qualunque consulenza legale produce raccomandazioni generiche.

Se vuoi accelerare

Echo accompagna le PMI italiane in questo percorso. Un AI Readiness Audit dura 2–3 settimane e produce: mappa strumenti, classificazione rischio, policy proporzionata, schede documentazione, formazione referenti. Poi se serve consulenza legale, sai esattamente dove chiamarla.

Contatti

Silvia Rinaldi — Founder, Echo S.r.l.

Email: info@echowebagency.it

Sito: echo.srl

Sede: Via Lelio e Fausto Socini 32/B, 42122 Reggio Emilia (RE)

Tel: +39 351 7027294

Trenta minuti di call gratuita: <https://calendly.com/echowebagency-info/formazione>

Approfondimenti correlati sul sito echo.srl:

- Servizio Governance AI: echo.srl/governance-ai
- AI Readiness Audit: echo.srl/ai-readiness-audit
- Articolo "Stai usando l'AI fuori legge": echo.srl/blog/stai-usando-ai-fuori-legge-ai-act-pmi
- Case study maison di alta maglieria: echo.srl/casi-studio/maison-knit-luxury

Questa pubblicazione è una guida operativa basata sull'esperienza diretta di Echo S.r.l. con PMI italiane manifatturiere, moda e beauty. Non sostituisce una consulenza legale qualificata. Tutte le informazioni sono aggiornate a giugno 2026.