

AI ACT

RIVOLUZIONE ONLINE – 09 FEBBRAIO 2026

[Aggiornamento maggio 2026](#). Il 7 maggio 2026 Parlamento europeo e Consiglio UE hanno raggiunto un accordo provvisorio sul Digital Omnibus, che rinvia al 2 dicembre 2027 gli obblighi per i sistemi ad alto rischio. L'accordo non è ancora legge definitiva. Restano invariati – e pienamente in vigore dal 2 agosto 2026 – gli obblighi di formazione del personale, trasparenza dei contenuti AI-generati e contrattualizzazione con i fornitori AI (DPA).

Chi usa intelligenza artificiale ha meno di 6 mesi per mettersi in regola.

In Europa è in vigore il primo regolamento al mondo sull'intelligenza artificiale.

Riguarda non solo gli sviluppatori, ma chiunque usi per lavoro ChatGPT o altre AI, generatori di immagini, chatbot o sistemi automatizzati.

Migliaia di aziende, studi professionali, associazioni e scuole usano strumenti di intelligenza artificiale ogni giorno per scrivere contenuti, generare immagini, rispondere ai clienti, selezionare candidati, automatizzare processi.

Molti lo fanno senza sapere che dal **2 agosto 2026** dovranno rispettare obblighi precisi stabiliti dall'[AI Act](#).

E che le sanzioni per chi non si adegua arrivano fino a 35 milioni di euro o al 7% del fatturato annuo; per le PMI si applica l'importo più basso tra i due, e il regime sanzionatorio pieno per i sistemi ad alto rischio è stato rinviato al 2027.

Chi deve preoccuparsi

Il regolamento riguarda **chiunque usi l'intelligenza artificiale in ambito professionale**.

Se nella nostra organizzazione qualcuno usa ChatGPT, Claude, Gemini o altri per scrivere testi, oppure Midjourney, DALL-E ecc. per generare immagini; se sul sito c'è un assistente virtuale; se facciamo screening di CV con funzioni "intelligenti" di automazione e analisi dati, siamo nel perimetro della norma.

Agosto 2026

L'AI Act è operativo da febbraio 2025, ma è dal 2 agosto 2026 che entrano in vigore gli obblighi più stringenti e le sanzioni pesanti.

Il regolamento classifica i sistemi in base al [rischio](#) che comportano, e questo **dipende dall'uso che facciamo dell'AI, non tanto dal settore dell'azienda**.

Ci sono infatti alcuni principi che valgono praticamente per tutti.

Ad esempio:

- **Trasparenza ed etichettatura**

Se pubblichiamo **contenuti creati con intelligenza artificiale** (testi, immagini, video) che potrebbero essere scambiati per contenuti reali o autentici, dobbiamo dichiararlo in modo chiaro. Stessa cosa se abbiamo un **chatbot AI** sul sito. Mentre un candidato il cui **cv** è valutato o selezionato da un sistema automatizzato deve capire come vengono prese le decisioni. Se nel nostro studio professionale o azienda inseriamo sull'AI **informazioni** del cliente **coperte da NDA**, stiamo violando l'accordo di riservatezza: rischiamo di perdere il cliente ed affrontare conseguenze legali.

- **Formazione del personale**

La **formazione** sull'AI è **obbligatoria**. Chi usa AI deve capire come funziona, quali sono i limiti, cosa può andare storto. Il nostro dipendente che carica dati personali sull'AI sta violando il GDPR, ma se nessuno glielo ha spiegato continuerà a farlo.

- **Supervisione umana**

L'AI può suggerire, proporre, aiutare, ma la decisione finale deve averla una **persona** che se ne assume la **responsabilità**. Nessuna decisione importante può essere presa dall'AI da sola.

- **Documentazione**

Serve tenere traccia di quali sistemi AI usiamo, per quali scopi, chi li ha autorizzati, chi è responsabile. Dobbiamo dimostrare di aver agito con **diligenza** se qualcosa va storto.

- **Valutazione dei rischi**

Prima di usare un sistema AI, bisogna chiedersi quali **danni** potrebbe causare.

Cosa fare ora

Dobbiamo dotarci di una [POLICY AI](#). Partire innanzitutto da una **mappatura** seria: inventariare tutti gli strumenti AI in uso (anche i plugin, le estensioni, ecc.).

Poi serve classificare per ogni strumento il livello di **rischio** e scrivere **regole** interne chiare: quali AI si possono usare e per cosa, quali dati è vietato caricare, chi controlla i risultati, chi è **responsabile** se qualcosa va storto.

Se usiamo l'AI per decisioni importanti, serve strutturare la **supervisione umana**.

Il punto di partenza immediato è senz'altro la **formazione** del personale, un obbligo già scattato a febbraio 2025. Oltre che un adempimento burocratico, formare i collaboratori è lo scudo più efficace per evitare che un errore umano (come caricare dati sensibili su un'AI pubblica) si trasformi in un disastro legale.

Perché non conviene aspettare

Le sanzioni arrivano fino a 35 milioni di euro o 7% del fatturato annuo.

Per le PMI si applica l'importo più basso tra i due, ma parliamo comunque di cifre che possono mettere in ginocchio la nostra organizzazione.

I primi contenziosi sono in corso e gli studi legali monitorano casi su uso improprio di intelligenza artificiale.

I danni non si limitano poi solo a una questione di multe.

La conformità all'AI Act diventerà requisito nelle **gare pubbliche** e nei **contratti** tra aziende: chi non sarà in regola si troverà escluso da molte opportunità.

Scuole e **organizzazioni** che inseriscono in un sistema AI dati apparentemente aggregati (statistiche su studenti, informazioni su beneficiari) spesso non si rendono conto che possono rendere identificabili i minori, violando importanti norme sulla **privacy**.

Il **personale** dell'azienda può rivalersi se non ha ricevuto la formazione obbligatoria. Un'autorità può ordinare di bloccare un sistema AI non conforme, costringendoci a **riorganizzare processi interi in emergenza**. E così via.

La compliance come opportunità

L'AI Act stabilisce degli obblighi, tuttavia formazione e compliance sono anche una occasione. Documentare le proprie pratiche, garantire trasparenza, dimostrare supervisione umana, diventano un **elemento distintivo**.

In settori dove la fiducia conta – sanità, educazione, servizi professionali, terzo settore – poter dire “i nostri processi AI sono conformi al regolamento europeo” è anche un vantaggio competitivo reale.

Molte organizzazioni stanno andando oltre gli adempimenti minimi, dotandosi di un [codice etico sull'uso dell'AI](#): un documento interno che definisce i principi guida e i valori che orientano le scelte tecnologiche.

Non è obbligatorio per legge, ma diventa un elemento di **trasparenza** verso clienti, partner e stakeholder.

L'Italia ha approvato la prima legge nazionale sull'AI in Europa ([legge 132/2025](#)), che integra il regolamento UE con regole specifiche.

L'Agenzia per l'Italia Digitale (AgID), l'Agenzia per la Cybersicurezza Nazionale (ACN) e il Garante per la protezione dei dati personali sono le autorità di vigilanza.

Abbiamo pochi mesi per metterci in regola.

Può sembrare tempo sufficiente, ma considerando che serve capire quali AI usiamo davvero, valutare i rischi, scrivere policy, formare il personale, organizzare i controlli e documentare tutto, non è poi così tanto.

L'**intelligenza artificiale** è uno strumento potente e utile.

Usarla con consapevolezza e trasparenza significa proteggere la propria organizzazione e le persone con cui lavoriamo.

– di Paola Furlan

Per approfondire

- [GOVERNANCE AI](#)
- [POLICY AI](#)
- [CODICE ETICO AI](#)
- [FORMAZIONE AI](#)