AVVERA

# AI Act in Azienda

## Guida Operativa 2026

*con gli aggiornamenti Digital Omnibus*
*e Legge italiana 23-9-2025 n.132*

**Note di revisione**

Questa è la versione aggiornata della Guida Operativa "AI Act in Azienda", pubblicata originariamente nel dicembre 2025.
L'aggiornamento si è reso necessario a seguito dell'approvazione definitiva del pacchetto "Digital Omnibus VII" (Regolamento di modifica dell'AI Act), approvato dal Parlamento europeo il 16 giugno 2026 e dal Consiglio dell'Unione europea il 29 giugno 2026, che modifica in modo significativo il calendario di applicazione e alcuni contenuti sostanziali del Regolamento (UE) 2024/1689 ("AI Act").

Le parti della guida aggiornate rispetto alla versione originale sono segnalate in blu.

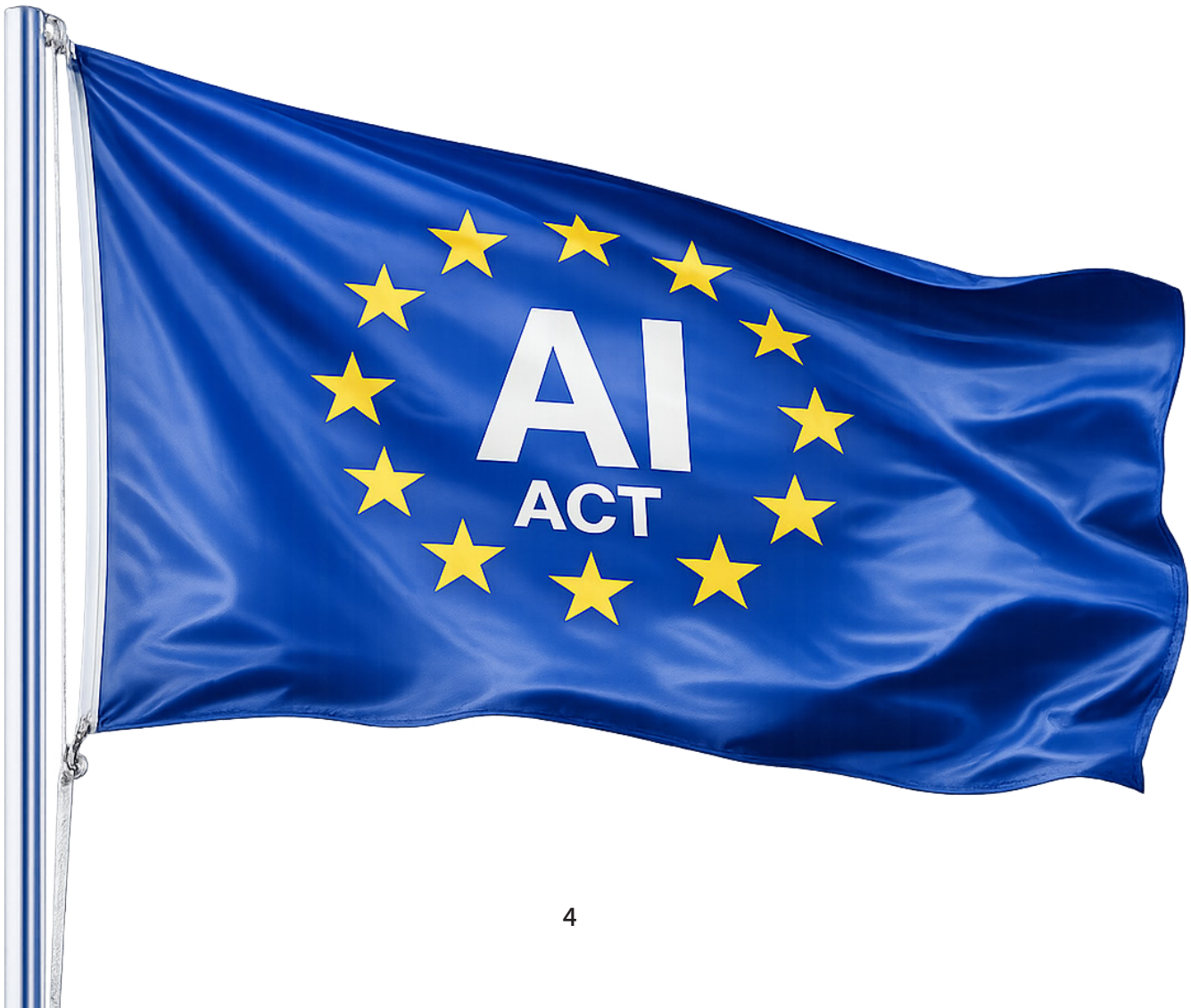
Tutti i contenuti non contrassegnati restano validi e non hanno subito modifiche sostanziali.
Due capitoli interamente nuovi sono stati aggiunti in chiusura del documento:

- IL DIGITAL OMNIBUS: COSA CAMBIA
  dedicato alle modifiche del Regolamento (UE) 2024/1689

- LA LEGGE ITALIANA 132/2025 SULL'INTELLIGENZA ARTIFICIALE
  dedicato al layer normativo nazionale che si affianca all'AI Act.

*Attenzione: alla data di redazione di questo aggiornamento (3 luglio 2026), il regolamento di modifica dell'AI Act risulta approvato sia dal Parlamento sia dal Consiglio UE ed entrerà in vigore decorsi 3 giorni dalla pubblicazione in Gazzetta Ufficiale dell'Unione Europea. Analogamente, i decreti attuativi della Legge 132/2025 sono in fase di approvazione (esame preliminare del Consiglio dei Ministri del 10 giugno 2026) e non hanno ancora completato l'iter parlamentare. Si raccomanda di verificare lo stato di avanzamento più recente prima di assumere decisioni operative vincolanti basate sulle nuove scadenze.*

# Sommario


AI
ACT

# Introduzione

L'Artificial Intelligence Act (AI Act) è il primo regolamento al mondo sull'uso dell'intelligenza artificiale. È entrato in vigore gradualmente a partire dal 2024 e stabilisce obblighi diversi in base al rischio dei sistemi AI. Questa guida è pensata per i nostri clienti come uno strumento pratico, comprensibile e immediatamente applicabile nell'organizzazione.

*Rispetto alla prima edizione, questa versione recepisce le modifiche introdotte dal pacchetto "Digital Omnibus VII", che ha rinviato alcune scadenze, introdotto nuovi divieti e semplificato alcuni adempimenti. Il quadro generale - approccio basato sul rischio, obblighi differenziati, tutela dei diritti fondamentali - resta invariato: cambiano principalmente i tempi e alcuni dettagli attuativi.*

## Obiettivi

- comprendere cosa richiede l'AI Act, nella sua versione aggiornata;
- identificare dove l'azienda utilizza l'AI (anche "nascosta");
- classificare i sistemi AI per livello di rischio;
- adottare checklist operative e modelli documentali;
- conoscere le nuove scadenze e le semplificazioni introdotte dal Digital Omnibus.


AI
Act

# AI Act, a chi si applica

**Si applica a:**

- fornitori di sistemi IA (chi li sviluppa o li commercializza);
- deployer/utilizzatori (le aziende che li implementano);
- importatori, distributori, integratori.

**Punti chiave:**

- Si applica anche all'AI sviluppata fuori dall'UE ma utilizzata nell'UE.
- Prevede un approccio risk-based, confermato e non modificato nella sua impostazione dal Digital Omnibus.

# Obiettivi dell'AI ACT

L'AI Act nasce con l'ambizione dichiarata di creare il primo quadro normativo organico al mondo per regolare l'intelligenza artificiale, con un equilibrio complesso: promuovere l'innovazione e proteggere i diritti fondamentali.
Per comprenderne la logica e per applicarlo correttamente in azienda è fondamentale cogliere le finalità che hanno guidato il legislatore europeo. Il Digital Omnibus non modifica questi obiettivi, ma ne rende più graduale e realistica l'attuazione.

**1. Tutelare i diritti fondamentali e i valori dell'UE**
L'obiettivo primario è garantire che l'AI sia sviluppata e utilizzata in modo da preservare i diritti delle persone, in particolare:

- diritto alla non discriminazione;
- protezione dei dati personali;
- dignità umana;
- libertà di espressione e informazione;
- libertà professionale e diritto al lavoro;
- tutela dei consumatori.

**Traduzione operativa in azienda**
- introdurre controlli su bias e discriminazioni;
- fornire trasparenza su modelli e decisioni automatizzate;
- garantire sempre una supervisione umana nei casi critici.

# Obiettivi dell'AI Act

### 2. Rafforzare la sicurezza dei Sistemi AI

L'AI Act mira a prevenire rischi legati a:
- malfunzionamenti;
- vulnerabilità cybersecurity;
- manipolazioni intenzionali;
- effetti imprevedibili dei modelli.

Traduzione operativa
- logging e tracciabilità;
- stress test periodici;
- audit tecnici;
- requisiti di robustezza e resilienza.

*Il Digital Omnibus alleggerisce l'approccio originariamente previsto per il post-market monitoring dei sistemi high-risk: al posto di un "implementing act" vincolante con template obbligatorio, la Commissione pubblicherà linee guida non vincolanti (attese entro il 2 settembre 2027), lasciando alle aziende maggiore flessibilità nell'adattare il monitoraggio alla natura del proprio sistema.*

### 3. Creare fiducia nell'adozione dell'AI

La percezione di rischio, opacità o imprevedibilità dell'AI rischia di ostacolare l'innovazione. L'AI Act vuole creare un ambiente di fiducia, affinché cittadini e imprese possano usare l'AI senza timori.

Traduzione operativa
- informative chiare;
- governance interna ben definita;
- certificazione e conformità verificabili;
- processi documentati per ogni sistema AI.

### 4. Promuovere l'innovazione e la competitività della UE

L'obiettivo non è affatto "frenare l'AI". Al contrario, il regolamento:
- crea un quadro stabile e prevedibile per gli investimenti;
- introduce sandbox normative per sperimentare in sicurezza;
- riduce i rischi legali per le aziende che adottano processi di conformità.

Traduzione operativa
- possibilità di partecipare a sandbox regolatorie;
- utilizzo della compliance come elemento competitivo e di branding;
- sviluppo di AI interne con criteri "by design" conformi al mercato.

*Il termine per l'istituzione, da parte delle autorità nazionali competenti, dei sandbox normativi per l'IA è stato posticipato dal 2 agosto 2026 al 2 agosto 2027.*

### 5. Armonizzare il quadro normativo europeo

L'AI Act evita la frammentazione regolatoria tra Stati Membri, garantendo un mercato unico dell'AI, con regole condivise per fornitori, integratori, utilizzatori, distributori e modelli generici (GPAI).

Traduzione operativa
- semplificazione per le aziende multinazionali;
- possibilità di utilizzare sistemi AI uniformemente in tutti i paesi UE;
- riduzione dei costi di compliance multipaese.

*Il Digital Omnibus estende molte delle semplificazioni finora riservate alle micro, piccole e medie imprese (PMI) anche alle "piccole imprese a media capitalizzazione" (small mid-cap), incluse le facilitazioni sulla documentazione tecnica e sul sistema di gestione della qualità.*

### 6. Prevenire usi distorti o abusivi dell'AI

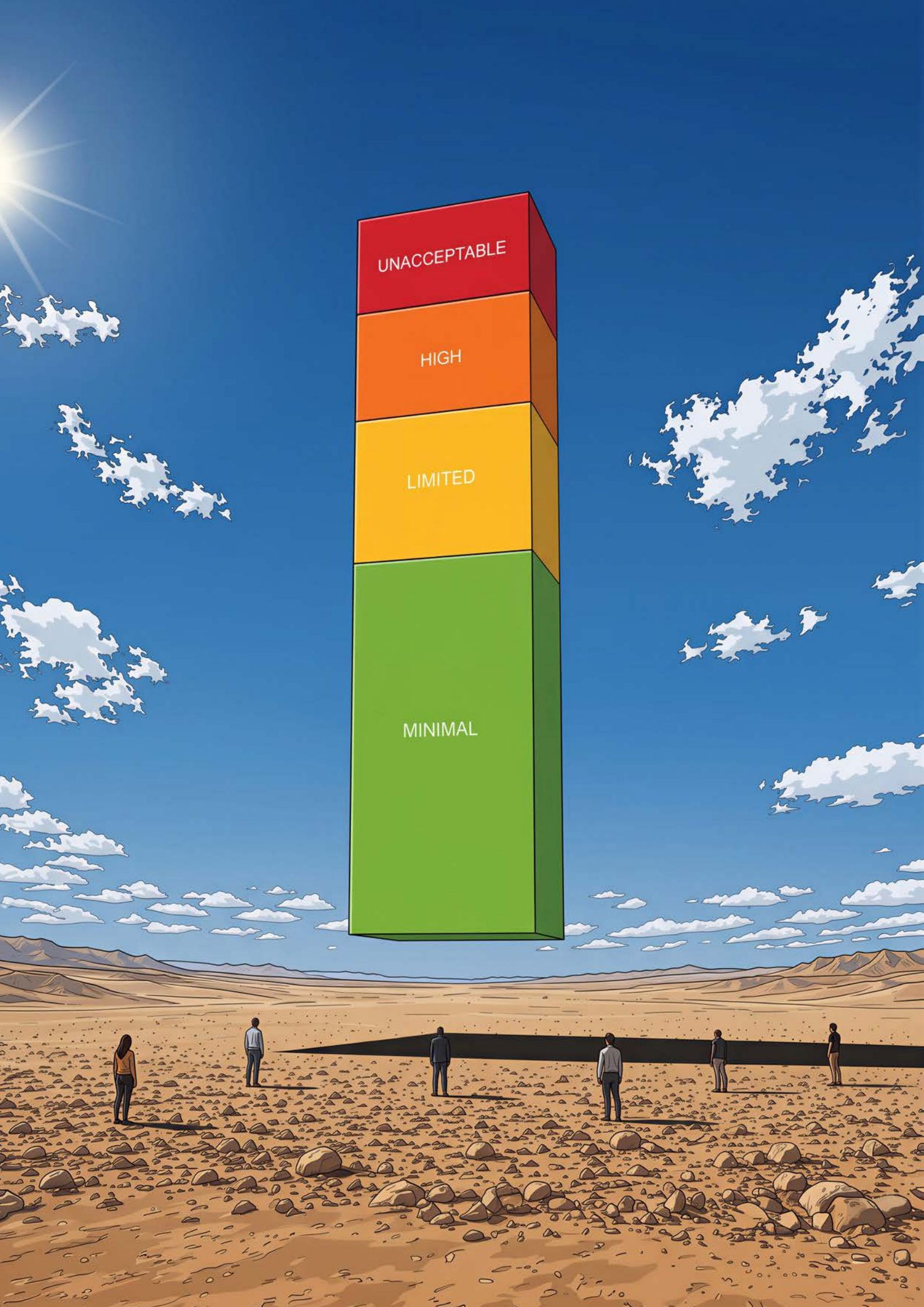
L'AI Act individua categorie vietate per contrastare sorveglianza massiva, manipolazione subliminale, social scoring e sfruttamento delle vulnerabilità.

Traduzione operativa
- valutare attentamente casi d'uso borderline;
- predisporre un comitato etico interno per l'approvazione dei casi d'uso;

### 7. Garantire trasparenza e responsabilità

L'obiettivo è assicurare che le aziende sappiano cosa fa il sistema AI, che i cittadini possano essere informati adeguatamente e che le decisioni critiche non siano "scatole nere".

Traduzione operativa
- definizione di accountability interna;
- policy che definiscono ruoli e responsabilità;
- strumenti di explainability e reporting.


UNACCEPTABLE
HIGH
LIMITED
MINIMAL

# Classificazione dei rischi

**A) Rischio Inaccettabile ( vietato )**

- social scoring generalizzato;
- manipolazione subliminale;
- sfruttamento delle vulnerabilità;
- riconoscimento biometrico in tempo reale in spazi pubblici (salvo eccezioni);
- biometria ex-post su larga scala;
- database biometrici tramite scraping massivo;
- categorizzazione biometrica su caratteristiche sensibili;
- emotion recognition nelle scuole e sul lavoro;
- polizia predittiva basata su profiling;
- manipolazione politica di gruppi elettorali.

- *NUOVO - sistemi di "nudificazione":*
  *sistemi progettati per generare o manipolare immagini, video o audio sessualmente espliciti raffiguranti persone identificabili senza il loro consenso (c.d. nudifier tool);*

- *NUOVO - materiale pedopornografico sintetico:*
  *sistemi idonei a produrre materiale di abuso sessuale su minori generato artificialmente. Il divieto si applica anche ai deployer che impiegano tali sistemi a questo scopo.*

**Esito: divieto assoluto**
I divieti "storici" sono già pienamente in vigore dal 2 febbraio 2025.
I due nuovi divieti introdotti dal Digital Omnibus si applicano invece dal 2 dicembre 2026: le imprese hanno tempo fino a tale data per adeguare i propri sistemi.

## Classificazione dei rischi

**B) Alto Rischio ( High Risk )**

**Due categorie:**

- AI come componente di sicurezza (es. robotica industriale, dispositivi medici).
- AI impiegata in settori critici: HR e selezione del personale; valutazione creditizia; gestione infrastrutture critiche; giustizia e law enforcement; educazione e formazione professionale; accesso e valutazione di servizi essenziali e pubblici; migrazione, asilo e controllo delle frontiere; amministrazione della giustizia e processi democratici.

**Cosa NON è High-Risk (chiarimenti utili per le aziende)**
Non rientrano automaticamente nel rischio alto:

- chatbot generativi > rischio limitato;
- strumenti di marketing predittivo > basso/medio rischio;
- sistemi di automazione generica;
- AI che assiste ma non decide in modo significativo.

La soglia determinante è se l'AI influisce significativamente su diritti, accesso a servizi o sicurezza fisica.

*Il Digital Omnibus ha inoltre chiarito la definizione di "componente di sicurezza" (modifica del punto 14, art. 3 AI Act): i prodotti dotati di funzioni IA che si limitano ad assistere l'utente o a ottimizzare le prestazioni non sono automaticamente soggetti agli obblighi high-risk, se un loro guasto o malfunzionamento non comporta rischi per la salute o la sicurezza fisica delle persone.*

**Esito: forti obblighi di compliance.**

*Le date di applicazione sono state modificate dal Digital Omnibus (in luogo dell'originario 2 agosto 2026):*
*2 dicembre 2027 per i sistemi di IA ad alto rischio autonomi (stand-alone, Allegato III);*
*2 agosto 2028 per i sistemi di IA ad alto rischio integrati come componenti di sicurezza in prodotti disciplinati da normativa settoriale UE (Allegato I).*

*
Si tratta di date "di backstop". Se la Commissione europea certifica con apposita decisione la disponibilità di norme armonizzate, specifiche comuni o linee guida adeguate, l'applicazione potrà scattare anticipatamente: 6 mesi dopo la decisione per i sistemi dell'Allegato III, 12 mesi dopo per quelli dell'Allegato I. È quindi opportuno monitorare periodicamente gli aggiornamenti della Commissione, senza fare affidamento esclusivo sulle date del 2027/2028 come termine ultimo di sicurezza.

# Classificazione dei rischi

## C) Rischio Limitato

I sistemi a rischio limitato non hanno impatti significativi sulla sicurezza o sui diritti fondamentali, ma possono generare rischi legati a trasparenza, comprensione dell'utente o potenziali manipolazioni.

Esempio: sistemi che interagiscono con l'utente (es. chatbot, assistenti virtuali sui siti web, tool LLM che rispondono automaticamente ai clienti, generatori di deepfake non fraudolenti, ecc.).

**Esito: obblighi di trasparenza**
l'utente deve sapere chiaramente e prima dell'interazione che sta interagendo con un sistema di AI.

*Gli obblighi di trasparenza generale (comunicare che si sta interagendo con un'IA) sono già in vigore. Tuttavia, per lo specifico obbligo di etichettatura/marcatura dei contenuti sintetici (immagini, audio, video generati o modificati dall'IA - c.d. watermarking), il Digital Omnibus ha ridotto il periodo di tolleranza da 6 a 3 mesi, fissando la scadenza effettiva al 2 dicembre 2026. Le imprese che utilizzano già sistemi di IA generativa devono quindi considerare prioritario l'adeguamento tecnico a questo obbligo.*

**Sistemi a Rischio Limitato - cosa fare subito (art. 50–52)**

- Dichiarare che l'utente interagisce con un'AI.
- Etichettare contenuti generati, modificati o sintetici - con scadenza al 2 dicembre 2026 per il watermarking tecnico.
- Garantire che l'utente possa comprenderlo facilmente.
- Usare interfacce trasparenti (no dark patterns).
- Formare il personale sul corretto uso dei tool AI generativi.

# Classificazione dei rischi

**D) Rischio Minimo**

I sistemi a rischio minimo costituiscono la categoria più ampia dell'AI Act. Comprendono la maggior parte degli usi aziendali "ordinari" dell'intelligenza artificiale che non incidono sui diritti fondamentali e non comportano rischi significativi per la sicurezza.

Esempi tipici:
- strumenti di AI incorporati nel software comune (funzioni intelligenti in produttività office)
- modelli per analytics non utilizzati per decisioni su persone; sistemi di clustering
- segmentazione o forecasting non impattanti su diritti; filtri antispam
- suggerimenti automatici non decisivi
- sistemi generativi usati solo per brainstorming o creatività interna.

Per questi sistemi non ci sono obblighi specifici né vincoli di conformità.

**Rischio minimo non significa rischio trascurabile**
Anche se non vi sono obblighi formali, l'azienda dovrebbe:

- evitare un uso "non controllato" che possa sconfinare in processi sensibili;
- valutare periodicamente se cambiano finalità o perimetro d'uso;
- mantenere un livello basico di tracciabilità.

# Obblighi per le Aziende

Gli obblighi cambiano in funzione della categoria di rischio del sistema AI: Inaccettabile, Alto, Limitato, Minimo. L'obiettivo è guidare l'azienda a usare l'AI in modo sicuro, trasparente e conforme.

## Obblighi generali per tutte le aziende

- Classificare tutti i sistemi AI presenti in azienda secondo la loro categoria di rischio.
- Adottare una policy aziendale AI.
- Formare il personale sulla gestione dei rischi.
- Stabilire un AI Governance Team (o esternalizzarlo).

## Obblighi specifici per categoria di rischio

| Categoria | Obblighi principali | Note operative (aggiornate) |
|---|---|---|
| Inaccettabile | Vietati (incl. nudifier tool e CSAM sintetico, dal 2/12/2026) | Nessun uso consentito; sanzioni immediate se utilizzati |
| Alto Rischio | Documentazione tecnica completa (Art. 8-11); AI Impact Assessment (AIA/FRIA); gestione rischio e mitigazioni; registrazione UE; logging e audit; human oversight | Applicazione dal 2/12/2027 (sistemi autonomi) o 2/8/2028 (componenti di sicurezza) - salvo anticipazione da parte della Commissione. FRIA assorbibile nella DPIA. |
| Rischio Limitato | Trasparenza verso utenti (Art. 50-52); disclosure di contenuti generati o sintetici; interfacce chiare e comprensibili | Trasparenza generale già in vigore; watermarking tecnico dei contenuti sintetici con scadenza al 2/12/2026 |
| Rischio Minimo | Nessun obbligo legale specifico | Buone pratiche: mappare sistemi, monitorare evoluzioni, formazione base del personale |

## Rischio Inaccettabile

- Uso vietato (Art. 5).
- Sistemi come social scoring per bonus/penalità, sorveglianza biometrica in tempo reale in luoghi pubblici, AI manipolativa subliminale - già in vigore, qualsiasi utilizzo comporta sanzioni immediate.
- *NUOVO: nudifier tool e sistemi di generazione di materiale pedopornografico sintetico - vietati dal 2 dicembre 2026.*

# Obblighi per le aziende

**Alto Rischio**

Obblighi dettagliati (Art. 6-15, Allegato III): documentazione tecnica completa (architettura, dati, limiti); valutazione del rischio (AI Impact Assessment); logging, audit e tracciabilità delle decisioni; supervisione umana (human oversight); registrazione dei sistemi in un database UE. Esempi: screening CV automatico, scoring creditizio, sistemi sanitari, infrastrutture critiche.

- *Le scadenze sono ora il 2 dicembre 2027 (sistemi autonomi) e il 2 agosto 2028 (componenti di sicurezza in prodotti regolati), salva anticipazione della Commissione europea.*
- *La Valutazione di impatto sui diritti fondamentali (FRIA, art. 27) potrà essere assorbita nella DPIA ex GDPR quando i contenuti coincidono; la Commissione sta sviluppando un template e un tool automatizzato dedicati.*
- *È consentito, con adeguate garanzie, il trattamento di categorie particolari di dati personali ai fini del rilevamento e della correzione di bias, sia per i provider sia per i deployer.*
- *Semplificata la registrazione di alcuni sistemi high-risk (Allegato VIII, sezione B); resta però reintrodotto l'obbligo di registrazione anche per i fornitori che ritengono il proprio sistema esentato dalla qualifica di "alto rischio", a fini di maggiore tracciabilità sul mercato.*
- *Chiarito il rapporto con la normativa di prodotto (es. Regolamento Macchine, dispositivi medici, giocattoli, ascensori, imbarcazioni): non sono richiesti doppi adempimenti quando la normativa settoriale garantisce già un livello equivalente di tutela della salute e sicurezza.*

# Obblighi per le aziende

## Rischio Limitato

Obblighi principali (Art. 50-52):

- trasparenza verso gli utenti (comunicare che si sta interagendo con un'AI);
- disclosure dei contenuti generati o sintetici;
- interfacce chiare e comprensibili.

Esempi:
chatbot generativi, LLM per supporto redazionale, sistemi di raccomandazione.

*Il periodo di tolleranza per l'obbligo di etichettatura/marcatura (watermarking) dei contenuti generati da IA è ridotto da 6 a 3 mesi, con scadenza al 2 dicembre 2026.*

## Rischio Minimo

Nessun obbligo legale specifico (Art. 2, Considerandi 70-72).

Buone pratiche consigliate:
- mappare i sistemi
- monitorarne l'evoluzione
- formare il personale.

Esempi:
strumenti di produttività office, analisi interne non decisionali, filtri antispam.

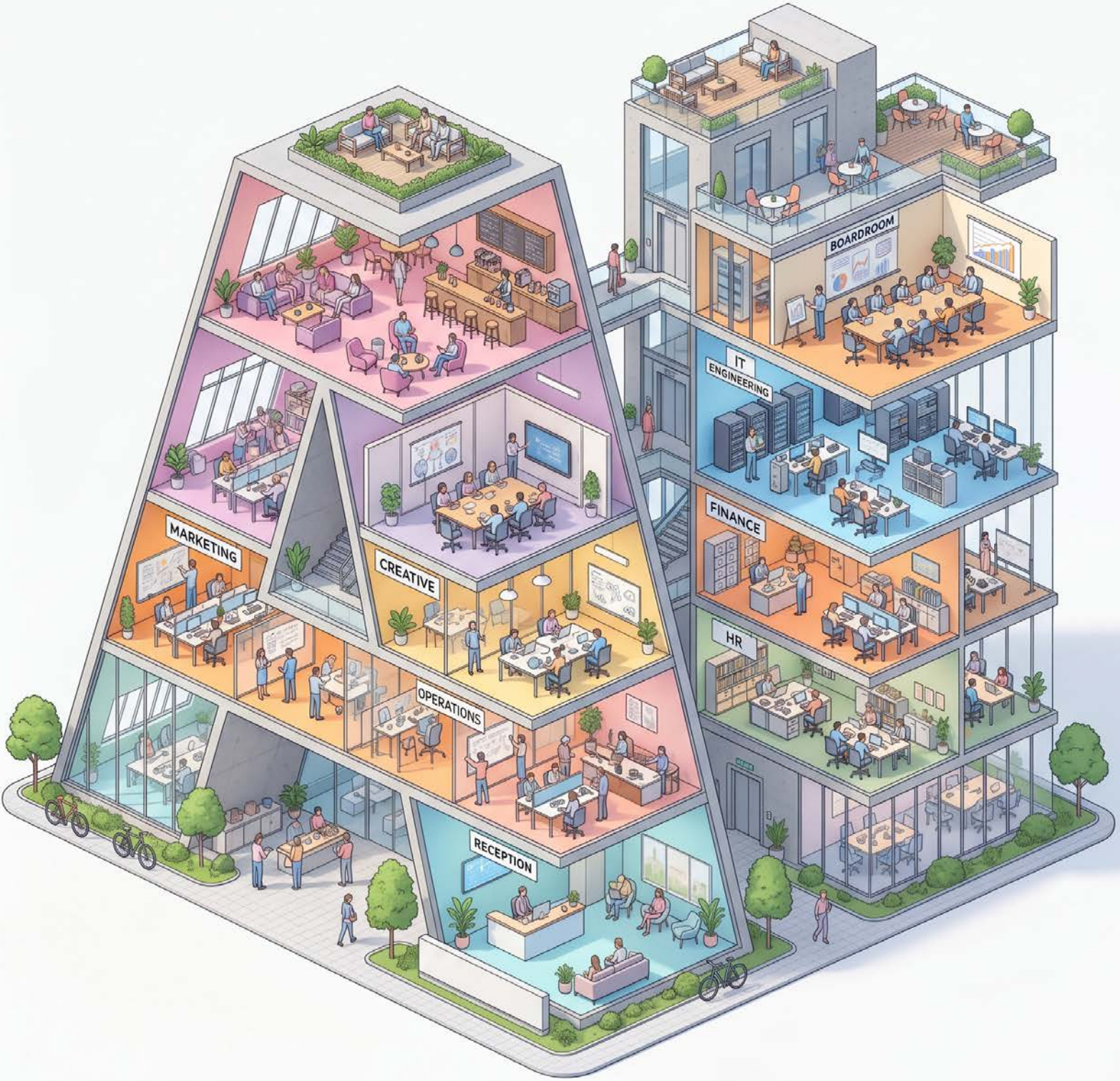
29R
06
06
79L
12
12
30

# Obblighi per l'uso di modelli GPAI / Foundation Models

Quando un'azienda integra modelli general purpose AI (GPAI):

- Verificare la documentazione fornita dal fornitore (architettura, dati di addestramento, policy d'uso).
- Valutare rischi operativi (allucinazioni, bias, vulnerabilità).
- Garantire trasparenza verso utenti e dipendenti se il modello interagisce con persone.
- Adottare policy interne di uso responsabile.
- Se il modello è integrato in processi critici, classificare il sistema come High-Risk e applicare tutti gli obblighi del Capo II.

I*l Digital Omnibus rafforza i poteri dell'AI Office (art. 75), attribuendogli competenza esclusiva sulla supervisione dei sistemi basati su modelli GPAI quando provider del modello e del sistema coincidono, nonché sui sistemi integrati in piattaforme online o motori di ricerca di dimensioni molto grandi (VLOP/ VLOSE, in coordinamento con il Digital Services Act), con possibilità di effettuare direttamente valutazioni di conformità prima dell'immissione sul mercato.*
*Restano competenti le autorità nazionali per i settori delle forze dell'ordine, gestione delle frontiere, autorità giudiziarie e istituti finanziari.*
*Per le aziende che integrano GPAI di grandi provider, questo significa un interlocutore centralizzato a livello europeo per le questioni di supervisione più complesse.*


BOARDROOM
IT
ENGINEERING
FINANCE
HR
MARKETING
CREATIVE
OPERATIONS
RECEPTION

# Come identificare l'AI in Azienda

Molte aziende usano l'AI senza saperlo. L'AI Act si applica anche ai modelli integrati in software di terze parti.

**Dove guardare:**

- Software HR (ATS, screening CV automatizzato).
- Tool di marketing (profilazione, lead scoring).
- ERP con moduli predittivi.
- Sistemi di controllo qualità in fabbrica (vision AI).
- CRM con suggerimento next-best-action.
- Soluzioni cloud che integrano LLM (Microsoft Copilot, Google Duet, ecc.).

**Definizione operativa di AI**
Secondo l'AI Act, si considera AI qualsiasi sistema che:

- utilizza algoritmi o modelli per prendere decisioni, supportare decisioni o generare output;
- apprende dai dati (machine learning, deep learning, NLP, CV, ecc.);
- simula capacità umane (ragionamento, linguaggio, riconoscimento immagini, generazione contenuti).

Esempio:
anche strumenti di previsione automatica, chatbot, generatori di contenuti o software di raccomandazione rientrano nella definizione di AI.

**Passaggi pratici per l'identificazione**

- **1. Mappatura dei processi aziendali**
  Elencare tutte le aree aziendali che usano software digitale: HR, marketing, customer care, produzione, finanza, R&D. Per ogni processo, chiedersi: "Viene preso qualche output decisionale o predittivo dall'AI?"

- **2. Inventario dei sistemi**
  Registrare tutti i software, tool, piattaforme e modelli integrati. Includere anche strumenti cloud e SaaS, add-on, plugin o modelli integrati in applicazioni esistenti.

## Come identificare l'AI in Azienda

- **3. Verifica dell'uso dell'AI**
  Identificare se il software genera output autonomi, raccomandazioni o decisioni. Controllare se usa tecniche di machine learning, deep learning, NLP o modelli generativi. Coinvolgere team IT, sicurezza e data science per confermare la presenza di componenti AI.

- **4. Classificazione preliminare**
  Per ciascun sistema AI identificato, fare una prima classificazione del rischio: Inaccettabile, Alto, Limitato o Minimo.
  Questo aiuta a determinare i successivi obblighi normativi e le relative scadenze aggiornate.

# Come identificare l'AI in Azienda

## Strumenti pratici per l'identificazione

- **Questionario interno AI** per dipartimenti e team: chiedere quali strumenti utilizzano, output generati e finalità.
- **Audit tecnico**: analizzare log, API, modelli integrati e librerie utilizzate.
- **Coinvolgimento dei fornitori**: richiedere informazioni sui sistemi AI forniti (ad esempio LLM, modelli generativi, soluzioni predittive).
- **Software di inventario IT**: integrare informazioni sull'uso di modelli AI.

## Buone pratiche operative

- Documentare tutti i sistemi identificati in un registro AI interno.
- Aggiornare periodicamente l'inventario per includere nuove integrazioni o aggiornamenti di modelli.
- Creare un responsabile interno AI per garantire supervisione, gestione rischi e compliance.
- Collegare l'inventario alla classificazione dei rischi e agli obblighi normativi.

## Esempi pratici per funzione aziendale

Per capire concretamente come l'AI può essere presente in azienda, è utile guardare funzione per funzione i possibili casi d'uso, con la relativa categoria di rischio e gli obblighi principali previsti dall'AI Act.

### Risorse Umane (HR)

In ambito HR, l'AI viene spesso utilizzata per screening dei candidati, analisi delle performance dei dipendenti o gestione delle FAQ tramite chatbot.

- Lo screening automatico dei CV è considerato un sistema ad alto rischio. Richiede documentazione tecnica completa, AI Impact Assessment e supervisione umana per ridurre il rischio di bias (obblighi pienamente esigibili dal 2 dicembre 2027).
- L'analisi delle performance dei dipendenti rientra spesso nella categoria rischio limitato, con l'obbligo principale di trasparenza verso i dipendenti.
- I chatbot HR rientrano in rischio limitato, con l'obbligo di informare gli utenti che stanno interagendo con un'AI.

### Marketing e Vendite

In marketing e vendite, l'AI supporta la personalizzazione delle campagne, la generazione automatica di contenuti e l'analisi predittiva delle vendite.

## Come identificare l'AI in Azienda

- I sistemi di raccomandazione prodotti e i chatbot di supporto marketing sono a rischio limitato: obbligo di trasparenza sui contenuti generati e, se sintetici (immagini/audio/video), obbligo di watermarking tecnico dal 2 dicembre 2026.
- L'analisi predittiva delle vendite rientra nel rischio minimo, senza obblighi legali specifici.

**Customer Care**
Nel servizio clienti, l'AI è spesso impiegata per chatbot, analisi dei sentiment dei clienti e risposta automatica ai ticket.

- I chatbot GPT-like rientrano nel rischio limitato: occorre informare l'utente e garantire trasparenza sui contenuti generati.
- L'analisi dei sentiment e la risposta automatica ai ticket sono generalmente a rischio minimo.

**Produzione e Operations**
In produzione, l'AI viene impiegata per manutenzione predittiva, ottimizzazione della logistica e robotica autonoma.

- Manutenzione predittiva e supply chain: rischio minimo.
- Robotica autonoma con supervisione umana: può essere alto rischio; se integrata come componente di sicurezza in macchinari, verificare l'eventuale esenzione da doppi adempimenti grazie al coordinamento con il Regolamento Macchine introdotto dal Digital Omnibus.

**Finanza e Controllo**
In ambito finanziario, l'AI supporta il credit scoring, la prevenzione delle frodi e l'analisi predittiva.

- Scoring creditizio e prevenzione frodi: High-Risk, soggetti a tutti gli obblighi di compliance (con le nuove scadenze 2027/2028).
- Analisi predittiva dei fatturati: rischio minimo.

**Ricerca e Sviluppo (R&D)**
Nel reparto R&D, l'AI è spesso utilizzata per generare prototipi, simulazioni o design creativo.

- Generazione di prototipi o design AI-generated: rischio minimo o limitato, con obblighi di trasparenza se i risultati vengono condivisi esternamente.
- Simulazioni critiche per la sicurezza: possono essere High-Risk.

**Buone pratiche trasversali**

- Tutti i sistemi AI devono essere mappati in un registro interno e classificati per categoria di rischio.
- È fondamentale formare il personale sull'uso responsabile dei sistemi AI.
- Occorre monitorare periodicamente le performance e i rischi, soprattutto per i sistemi generativi e quelli ad alto rischio, tenendo traccia delle scadenze aggiornate dal Digital Omnibus.

# Checklist operative

Questa checklist raccoglie i passaggi fondamentali per garantire che i sistemi AI aziendali siano identificati, classificati e gestiti in conformità con l'AI Act.

**Mappatura dei sistemi AI**
- Identificare tutti i sistemi AI presenti in azienda, inclusi software interni, SaaS, cloud e modelli esterni.
- Coinvolgere i reparti chiave (HR, Marketing, Customer Care, Produzione, Finanza, R&D) per avere una panoramica completa.

**Classificazione del rischio**
- Assegnare a ciascun sistema la categoria di rischio secondo l'AI Act: Inaccettabile, High-Risk, Limited-Risk o Minimal-Risk.
- Documentare la motivazione della classificazione, indicando la scadenza di conformità applicabile (2026 / 2027 / 2028 a seconda dei casi).

**Richiesta documentazione ai fornitori**
- Ottenere dettagli tecnici sui sistemi AI forniti: algoritmi, modelli utilizzati, misure di sicurezza, eventuali valutazioni di impatto già effettuate.

**Valutazione d'impatto AI (AI Impact Assessment / FRIA)**
- Applicare l'AIA/FRIA ai sistemi ad alto rischio, documentando potenziali impatti sui diritti fondamentali e le misure di mitigazione.
- Valutare se la FRIA può essere assorbita in una DPIA già predisposta ai sensi del GDPR.

**Definizione ruoli (AI Officer, IT, Legal, Risk Management)**
- Assegnare responsabilità chiare per gestione, supervisione e compliance dei sistemi AI.
- Garantire che ogni ruolo sappia quali obblighi normativi deve rispettare e con quali scadenze.

**Procedure di human oversight**
- Stabilire meccanismi di supervisione umana sui sistemi High-Risk e Limited-Risk critici.
- Definire responsabilità e modalità di intervento in caso di output AI problematici.

**Registro interno AI**
- Creare e mantenere aggiornato un registro con: nome del sistema AI; funzione aziendale associata; categoria di rischio; obblighi applicabili e relativa scadenza; documentazione tecnica disponibile; responsabile interno.

## Checklist operative

**Piano formazione dipendenti**

- Formare il personale sull'uso responsabile dei sistemi AI, sui rischi, sugli obblighi di trasparenza e sulle procedure interne.
- Aggiornare la formazione in base all'evoluzione dei sistemi e della normativa (incluse le modifiche del Digital Omnibus).

**Meccanismo per segnalazioni incidenti AI**

- Definire procedure interne per la gestione di errori, bias o malfunzionamenti dei sistemi AI.
- Garantire canali di segnalazione chiari e accessibili a tutti i dipendenti.

# Checklist per contratti con fornitori AI

Questa checklist aiuta a inserire nei contratti con fornitori di sistemi AI tutte le clausole necessarie per la compliance e la gestione dei rischi, secondo l'AI Act.

**Clausola di conformità all'AI Act**
- Inserire obbligo contrattuale che il fornitore garantisca la conformità dei sistemi AI alla normativa europea, incluse le modifiche introdotte dal Digital Omnibus.
- Prevedere che eventuali aggiornamenti normativi siano recepiti tempestivamente dal fornitore.

**Accesso a log e metriche**
- Garantire all'azienda il diritto di accesso ai log operativi e alle metriche dei sistemi AI.
- Assicurarsi che i dati forniti siano sufficienti per monitorare correttezza, bias e performance del modello.

**Audit e test congiunti**
- Prevedere la possibilità di condurre audit periodici e test congiunti dei sistemi AI.
- Stabilire modalità, frequenza e responsabilità per l'esecuzione di tali controlli.

**Obbligo di notificare vulnerabilità**
- Inserire clausola che obblighi il fornitore a segnalare tempestivamente eventuali vulnerabilità, malfunzionamenti o anomalie rilevate.
- Definire i tempi e le modalità di notifica e risoluzione.

**SLA di sicurezza**
- Definire Service Level Agreement chiari in termini di sicurezza, continuità operativa e risoluzione incidenti.
- Stabilire metriche, tempi di intervento e responsabilità per eventuali violazioni.

*NUOVO - clausola sul watermarking: per i fornitori di sistemi generativi, inserire l'impegno contrattuale a implementare le soluzioni tecniche di marcatura dei contenuti sintetici entro il 2 dicembre 2026.*

*NUOVO - clausola sulla registrazione UE: richiedere conferma scritta dell'avvenuta (o prevista) registrazione del sistema nella banca dati UE, anche quando il fornitore ritiene il sistema esente dalla qualifica di alto rischio.*

# Altre checklist

**Checklist per l'implementazione di nuovi sistemi AI**
Questa checklist è utile prima di introdurre un nuovo sistema AI in azienda. Aiuta a valutare rischio, obblighi normativi e impatti operativi:

- Analisi del caso d'uso e processo aziendale coinvolto.
- Classificazione del rischio AI secondo l'AI Act aggiornato.
- AI Impact Assessment / FRIA preliminare (verificando la possibilità di assorbimento nella DPIA).
- Verifica di conformità normativa e regolamentare, incluse le scadenze del Digital Omnibus.
- Definizione ruoli e responsabilità (AI Officer, IT, Legal, Risk Management).
- Pianificazione della supervisione umana (human oversight).
- Definizione di metriche e log per monitoraggio continuo.
- Procedure per test, validazione e revisione periodica del modello.

**Checklist di monitoraggio periodico dei sistemi AI**
Questa checklist serve per audit e controllo continuo dei sistemi già operativi, fondamentale soprattutto per HighRisk e Limited-Risk:

- Controllo aggiornamenti dei modelli e dei dataset.
- Verifica correttezza, bias e affidabilità dei risultati.
- Revisione dei log e delle metriche di performance.
- Controllo del rispetto degli obblighi di trasparenza verso utenti e dipendenti, incluso il watermarking.
- Aggiornamento registro interno AI.
- Valutazione necessità di AIA/FRIA aggiornata per High-Risk.

**Checklist per la gestione degli incidenti AI**
Indispensabile per garantire risposta rapida e gestione dei rischi:

- Identificazione e classificazione dell'incidente (errore, bias, malfunzionamento).
- Notifica interna ai responsabili (AI Officer, IT, Legal).
- Coinvolgimento del fornitore se necessario.
- Documentazione dell'incidente e azioni correttive.
- Comunicazione eventuale a stakeholder esterni (clienti, autorità - inclusa l'AI Office UE per i casi di sua competenza).
- Revisione procedure e aggiornamento piani di mitigazione.

# Altre checklist

**Checklist per l'uso dei modelli generativi / GPAI**
Data la crescente diffusione di foundation models, è utile avere linee guida dedicate:

- Verifica rischi potenziali di output non accurati o fuorvianti.
- Obbligo di disclosure quando i contenuti sono AI-generated, con marcatura tecnica entro il 2 dicembre 2026.
- Monitoraggio per bias o contenuti inappropriati.
- Definizione di limiti d'uso e supervisione umana.
- Registro degli utilizzi dei modelli generativi.
- Valutazione periodica dei modelli aggiornati.

**Checklist per la documentazione e audit esterni**
- Preparazione della documentazione tecnica richiesta dall'AI Act.
- Evidenziazione di misure di sicurezza, human oversight e mitigazione rischi.
- Disponibilità di log e metriche per audit esterni o ispezioni, anche da parte dell'AI Office UE per i sistemi di sua competenza.
- Aggiornamento dei registri e dei report di monitoraggio.

# Documentazione da implementare

Per garantire la conformità all'AI Act e la gestione efficace dei rischi, è fondamentale predisporre e mantenere aggiornata una serie di documenti interni, utili sia per l'audit interno sia per eventuali controlli esterni o ispezioni da parte delle autorità competenti.

**Registro dei sistemi AI**
Elenco completo di tutti i sistemi AI presenti in azienda, interni ed esterni (SaaS, cloud, modelli esterni). Per ogni sistema indicare: funzione aziendale; categoria di rischio (High-Risk, Limited-Risk, Minimal-Risk); obblighi normativi applicabili e relativa scadenza; responsabile interno; versione del modello e aggiornamenti.

**Documentazione tecnica dei sistemi AI**
- Dettagli su algoritmi, dataset utilizzati e metodologia di addestramento.
- Informazioni sul funzionamento del modello, limiti e potenziali rischi.
- Misure di sicurezza implementate e procedure di human oversight.
- Log e metriche operative necessarie per monitoraggio e audit.

**AI Impact Assessment (AIA/FRIA)**
- Valutazioni d'impatto per tutti i sistemi High-Risk.
- Analisi dei rischi per i diritti fondamentali, bias e discriminazioni.
- Misure di mitigazione e piani d'azione per ridurre i rischi.
- Aggiornamento periodico, soprattutto in caso di aggiornamenti dei modelli o cambiamenti del processo aziendale.
- Valutazione dell'eventuale assorbimento nella DPIA ex GDPR.

**Contratti e accordi con fornitori di AI**
- Clausole di conformità all'AI Act, aggiornate al Digital Omnibus.
- Obblighi di accesso a log e metriche.
- Audit e test congiunti.
- Obbligo di notificare vulnerabilità.
- SLA di sicurezza e continuità operativa.

**Procedure interne e linee guida**
- Procedure per supervisione umana (human oversight).
- Policy interne per uso responsabile dei sistemi AI.
- Linee guida su disclosure, trasparenza e gestione dei contenuti generati, incluso il watermarking tecnico.
- Piani di formazione dei dipendenti sull'uso dei sistemi AI e sui rischi associati.

## Documentazione da implementare

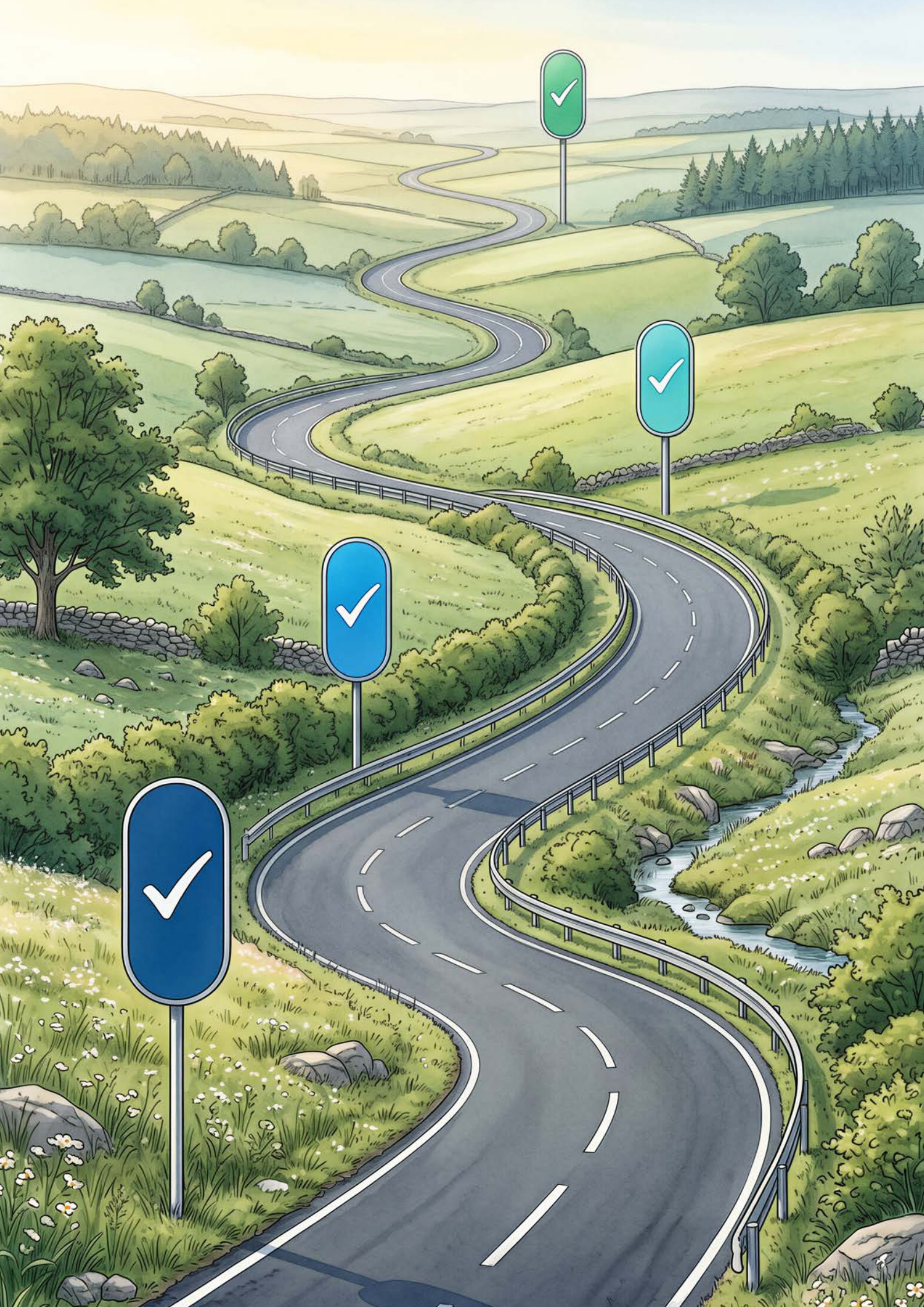
**Registrazione e gestione degli incidenti AI**

- Moduli o schede per la segnalazione di malfunzionamenti, bias o anomalie.
- Procedure di gestione e risoluzione degli incidenti.
- Log delle azioni correttive e dei follow-up.

**Audit e report periodici**

- Documentazione dei controlli periodici dei sistemi High-Risk e Limited-Risk.
- Report dei test, dei risultati di monitoraggio e delle eventuali azioni correttive.
- Registro dei miglioramenti implementati in seguito a audit interni o esterni.

*Suggerimento pratico: tutta la documentazione dovrebbe essere centralizzata e facilmente accessibile, idealmente in formato digitale, con versioning chiaro, per permettere aggiornamenti rapidi e audit efficienti - soprattutto in una fase, come quella attuale, di frequente evoluzione normativa.*

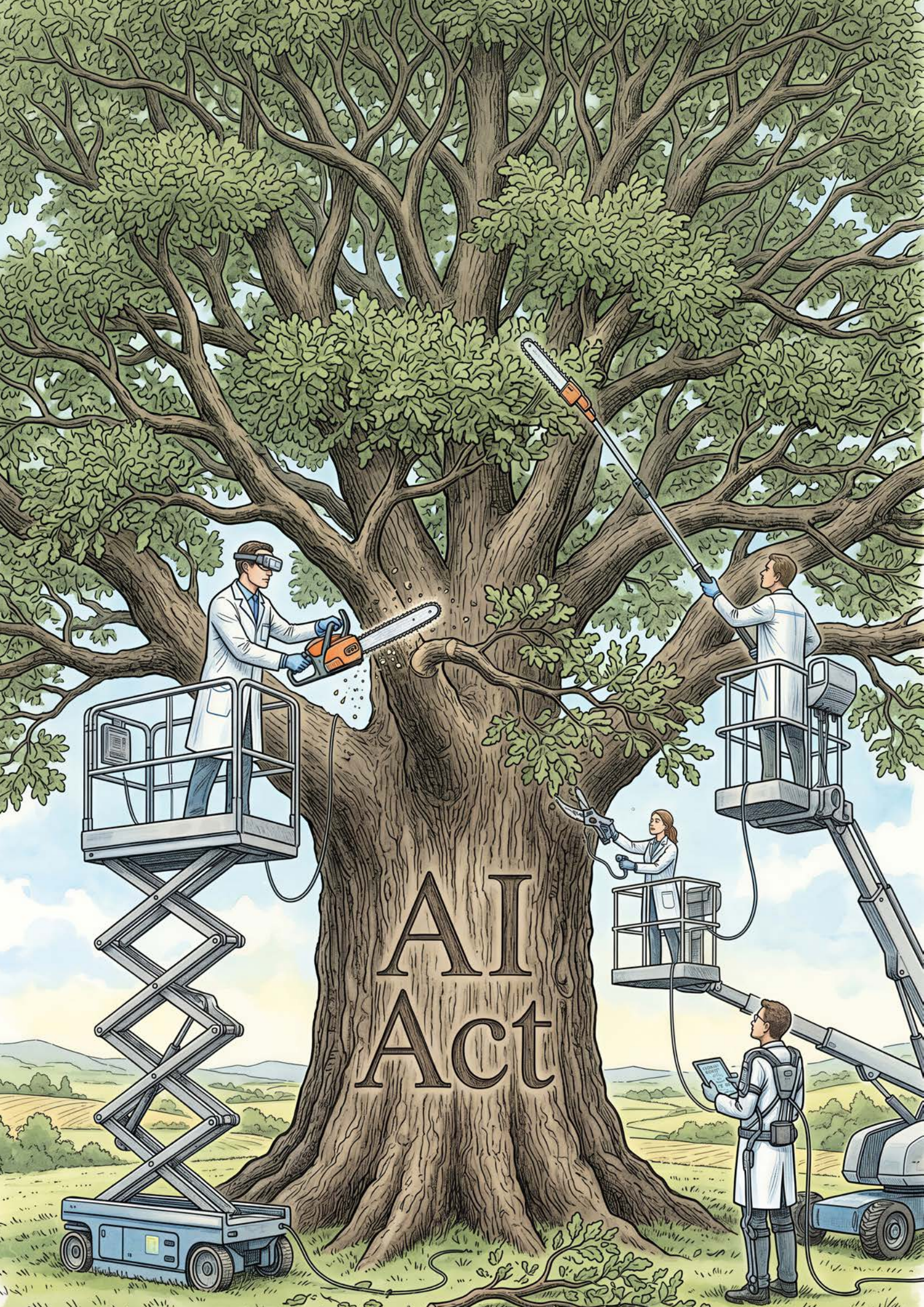


# Roadmap di adeguamento 2025-2028

*La roadmap originaria (2024-2026) è superata dalle modifiche introdotte dal Digital Omnibus. Di seguito la versione aggiornata delle scadenze principali.*

| Data | Obbligo / evento |
|---|---|
| 2 febbraio 2025 | Entrata in vigore dei primi divieti assoluti (Capi I e II, Art. 5 "storico"). |
| 2 agosto 2025 | Obblighi per i modelli GPAI / foundation models e per le autorità di governance nazionali. |
| 2 dicembre 2026 | Nuovi divieti su nudifier tool e materiale pedopornografico sintetico. Scadenza definitiva per l'obbligo di watermarking dei contenuti generati/sintetici (Art. 50). |
| 2 agosto 2027 | Termine per l'istituzione dei sandbox normativi nazionali per l'IA. |
| 2 settembre 2027 | Pubblicazione attesa delle linee guida (non vincolanti) della Commissione su post-market monitoring. |
| 2 dicembre 2027 | Obblighi per i sistemi di IA ad alto rischio AUTONOMI (Allegato III) — salvo anticipazione della Commissione (6 mesi da eventuale decisione). |
| 2 agosto 2028 | Obblighi per i sistemi di IA ad alto rischio integrati come componenti di sicurezza in prodotti regolati da normativa settoriale (Allegato I) — salvo anticipazione (12 mesi da eventuale decisione). |

*Le date del 2027 e del 2028 relative agli obblighi high-risk sono termini di backstop: la Commissione europea può farle scattare prima (6 o 12 mesi dopo un'apposita decisione), qualora ritenga disponibili standard tecnici e strumenti di supporto sufficienti. Si raccomanda quindi un monitoraggio periodico, e non un rinvio della pianificazione interna a ridosso delle scadenze massime.*


AI
Act

# Il Digital Omnibus: cosa cambia

*Capitolo aggiunto in sede di aggiornamento -Luglio 2026*

## 1. Cos'è il Digital Omnibus

Il "Digital Omnibus" (formalmente: pacchetto di semplificazione normativa n. VII) è un intervento orizzontale presentato dalla Commissione europea il 19 novembre 2025, con l'obiettivo dichiarato di ridurre gli oneri amministrativi, eliminare sovrapposizioni tra normative digitali diverse e rendere più realistico il calendario di applicazione di alcuni regolamenti - tra cui, per la parte che qui interessa, l'AI Act (Regolamento UE 2024/1689), oltre a GDPR, quadro cybersicurezza, identità digitale e data governance.

Il pacchetto si compone di più proposte regolamentari distinte; quella relativa all'AI Act è stata negoziata separatamente e ha seguito il seguente iter:

- 19 novembre 2025 - proposta della Commissione (COM/2025/836);
- 7 maggio 2026 - accordo politico provvisorio tra Parlamento europeo e Consiglio UE (trilogo);
- 16 giugno 2026 - approvazione definitiva del Parlamento europeo (423 voti favorevoli, 57 contrari, 174 astensioni);
- 29 giugno 2026 - approvazione del Consiglio dell'Unione europea;
- entrata in vigore prevista 3 giorni dopo la pubblicazione in Gazzetta Ufficiale dell'UE.

***Il testo non stravolge l'impianto dell'AI Act: l'approccio basato sul rischio (risk-based), le quattro categorie di rischio e gli obiettivi di tutela dei diritti fondamentali restano invariati. Cambiano soprattutto i tempi di applicazione, alcuni dettagli attuativi e - in senso restrittivo - l'elenco delle pratiche vietate.***

# Il Digital Omnibus: cosa cambia

## 2. Le nuove scadenze per i sistemi ad alto rischio

La modifica più rilevante per le aziende deployer riguarda il rinvio degli obblighi per i sistemi ad alto rischio (modifica dell'art. 113, lett. c dell'AI Act):

- *2 dicembre 2027 per i sistemi di IA ad alto rischio AUTONOMI (stand-alone), cioè quelli elencati nell'Allegato III che non fanno parte di un prodotto regolato da altra normativa di sicurezza UE (es. sistemi di screening CV, scoring creditizio, sistemi impiegati in ambito giudiziario o migratorio);*

- *2 agosto 2028 per i sistemi di IA ad alto rischio INTEGRATI come componenti di sicurezza in prodotti già disciplinati da normativa settoriale UE (es. dispositivi medici, macchinari, giocattoli, ascensori).*

*Questo posticipa di 16-24 mesi il termine originario, fissato al 2 agosto 2026. La ragione dichiarata è la mancanza, a oggi, di norme armonizzate, specifiche tecniche comuni e linee guida operative sufficientemente mature per consentire alle imprese e agli organismi notificati di conformarsi in modo affidabile.*

È importante comprendere il meccanismo "a doppio binario" introdotto:
È
- le date del 2 dicembre 2027 e del 2 agosto 2028 sono termini di backstop, cioè scadenze massime;
- se la Commissione europea, con apposita decisione, dichiara ufficialmente disponibili le norme armonizzate, le specifiche comuni o le linee guida necessarie, l'applicazione degli obblighi può scattare prima: 6 mesi dopo tale decisione per i sistemi dell'Allegato III, 12 mesi dopo per quelli dell'Allegato I.

**Conseguenza operativa:**
le aziende non dovrebbero considerare il 2027/2028 come un "si può rimandare tutto", ma continuare la pianificazione di compliance già avviata, monitorando gli annunci della Commissione che potrebbero anticipare l'entrata in vigore.

## 3. Nuovi divieti: nudifier tool e materiale pedopornografico sintetico

In controtendenza rispetto alla logica di semplificazione, il Parlamento europeo ha inserito nel testo un irrigidimento dell'art. 5 dell'AI Act (pratiche vietate), aggiungendo due nuove fattispecie di rischio inaccettabile:

- sistemi progettati per generare o manipolare immagini, video o audio sessualmente espliciti raffiguranti persone identificabili senza il loro consenso (i cosiddetti “nudifier tool”);
- sistemi idonei a produrre materiale di abuso sessuale su minori (CSAM) generato artificialmente.

Il divieto si applica non solo ai fornitori di tali sistemi, ma anche ai deployer che li impiegano per queste finalità. Le imprese avranno tempo fino al 2 dicembre 2026 per adeguare i propri sistemi e prodotti (ad esempio, disattivando funzionalità di editing immagini che potrebbero consentire questi utilizzi, o inserendo filtri e controlli tecnici).

*Le aziende che offrono strumenti di generazione o editing di immagini/video (anche in ambito marketing, gaming, entertainment) dovrebbero effettuare, entro la scadenza indicata, una verifica specifica su questo punto, poiché si tratta di un divieto assoluto per cui non sono previste eccezioni.*

### 4. Watermarking dei contenuti sintetici: scadenza anticipata

*Il periodo di tolleranza per l’obbligo di etichettatura tecnica (watermarking) dei contenuti generati o manipolati dall’IA - immagini, audio, video sintetici - è stato ridotto da 6 a 3 mesi. La nuova scadenza effettiva è fissata al 2 dicembre 2026, coincidente con quella dei nuovi divieti sopra descritti.*
*È inoltre stata introdotta una disciplina transitoria per i sistemi e i modelli che producono contenuti sintetici già immessi sul mercato prima del 2 agosto 2026, ai quali viene concesso un termine di adeguamento dedicato.*

Le aziende che utilizzano strumenti di IA generativa per la produzione di contenuti (marketing, comunicazione, customer care) devono considerare questa scadenza come prioritaria nella pianificazione 2026.

### 5. Semplificazioni per le imprese

**5.1 Estensione dei benefici PMI alle “small mid-cap”**
I benefici normativi già previsti per le micro, piccole e medie imprese vengono estesi anche alle “piccole imprese a media capitalizzazione” (small mid-cap), incluse le semplificazioni nella documentazione tecnica e nei requisiti del sistema di gestione della qualità.

**5.2 FRIA e DPIA: possibile assorbimento**
La Valutazione di impatto sui diritti fondamentali (FRIA, art. 27 AI Act) potrà essere assorbita nella DPIA già prevista dal GDPR (Regolamento (UE) 2016/679), quando i contenuti delle due

## Il Digital Omnibus: cosa cambia

valutazioni coincidono, evitando duplicazioni documentali. La Commissione europea sta sviluppando un template e uno strumento automatizzato per facilitare questo adempimento.

**5.3 Trattamento di dati per il rilevamento di bias**
Viene chiarita e agevolata, con adeguate garanzie, la possibilità per provider e deployer di trattare categorie particolari di dati personali (dati "sensibili" ex art. 9 GDPR) quando strettamente necessario per individuare e correggere distorsioni (bias) nei sistemi di IA ad alto rischio.

**5.4 Registrazione semplificata (ma non eliminata)**
Viene semplificata la procedura di registrazione di alcuni sistemi high-risk nella banca dati UE (Allegato VIII, sezione B). Attenzione però: il testo finale reintroduce l'obbligo di registrazione anche per i fornitori che ritengono il proprio sistema esentato dalla classificazione "alto rischio", con l'obiettivo di rafforzare la tracciabilità complessiva dei sistemi sul mercato europeo - un elemento di maggior onere, non di minore, rispetto alla proposta iniziale della Commissione.

**5.5 Coordinamento con la normativa di prodotto**
Viene chiarita l'interazione tra l'AI Act e le normative UE di sicurezza dei prodotti (in particolare il Regolamento Macchine, ma anche dispositivi medici, giocattoli, ascensori, imbarcazioni). I produttori di macchinari e prodotti che integrano IA come componente di sicurezza non dovranno affrontare duplicazioni di obblighi di conformità se la normativa settoriale garantisce già un livello equivalente di tutela della salute e della sicurezza. È inoltre stata chiarita la definizione di "componente di sicurezza" (modifica del punto 14, art. 3): i prodotti con funzioni IA che si limitano ad assistere l'utente o a ottimizzare le prestazioni, senza che un malfunzionamento comporti rischi per la salute o la sicurezza, non sono automaticamente soggetti agli obblighi high-risk. La Commissione dovrà inoltre redigere linee guida per assistere gli operatori dei sistemi high-risk disciplinati da normativa settoriale nel conformarsi ai requisiti dell'AI Act.

**5.6 Post-market monitoring più flessibile**
Anziché un "implementing act" vincolante con template obbligatorio e struttura standardizzata, la Commissione pubblicherà linee guida (guidance) non vincolanti, con un modello di riferimento non obbligatorio atteso entro il 2 settembre 2027. Le aziende potranno quindi adattare il piano di monitoraggio post-commercializzazione alla natura del proprio sistema, anziché seguire un formato imposto uniformemente.

**5.7 Sandbox normativi: più tempo per le autorità nazionali**
Il termine entro cui gli Stati membri devono istituire i sandbox normativi per l'IA (ambienti di sperimentazione controllata) è posticipato dal 2 agosto 2026 al 2 agosto 2027.

# Il Digital Omnibus: cosa cambia

## 6. Rafforzamento della governance: più poteri all'AI Office

Il regolamento modifica l'art. 75 dell'AI Act, attribuendo all'AI Office della Commissione europea competenza esclusiva per il monitoraggio e l'esecuzione degli obblighi riguardanti:

- i sistemi di IA basati su modelli GPAI, quando il fornitore del modello e quello del sistema coincidono;
- i sistemi integrati in piattaforme online o motori di ricerca di dimensioni molto grandi (VLOP/VLOSE), designati ai sensi del Digital Services Act, in coordinamento con quest'ultimo.

Per questi sistemi, l'AI Office potrà effettuare direttamente valutazioni di conformità prima dell'immissione sul mercato. Restano competenti le autorità nazionali per i settori delle forze dell'ordine, della gestione delle frontiere, delle autorità giudiziarie e degli istituti finanziari.
È inoltre prevista una semplificazione delle procedure di valutazione della conformità, con un percorso unificato di designazione degli organismi notificati, per evitare duplicazioni amministrative nell'ecosistema certificativo europeo.

## 7. Tabella di sintesi: cosa cambia rispetto alla prima edizione della guida

| Tema | Prima (versione 2025) | Ora (Digital Omnibus) |
|---|---|---|
| Obblighi highrisk autonomi | 2 agosto 2026 | 2 dicembre 2027 (backstop) |
| Obblighi high-risk componenti sicurezza | 2 agosto 2026 | 2 agosto 2028 (backstop) |
| Watermarking contenuti sintetici | Tolleranza 6 mesi | Tolleranza 3 mesi — scadenza 2/12/2026 |
| Divieti assoluti (Art. 5) | Elenco "storico" (social scoring, sorveglianza biometrica, ecc.) | + nudifier tool e CSAM sintetico dal 2/12/2026 |
| Sandbox normativi | Termine 2 agosto 2026 | Termine 2 agosto 2027 |
| FRIA | Valutazione autonoma obbligatoria | Assorbibile nella DPIA GDPR |
| Benefici PMI | Riservati a micro/piccole/medie imprese | Estesi anche alle small midcap |
| Post-market monitoring | Implementing act vincolante previsto | Linee guida non vincolanti (entro 2/9/2027) |
| Supervisione GPAI/VLOP | Non specificamente disciplinata | Competenza centralizzata AI Office |

# Il Digital Omnibus: cosa cambia

## 8. Cosa fare adesso — raccomandazioni operative

- **Non sospendere i progetti di compliance in corso.**
  Il rinvio delle scadenze high-risk al 2027/2028 non equivale a un rinvio indefinito: sono termini di backstop e la Commissione può anticiparli. Le aziende con sistemi high-risk dovrebbero mantenere il piano di adeguamento, eventualmente rimodulando le priorità temporali.

- **Dare priorità immediata al 2 dicembre 2026.**
  È la scadenza più vicina e riguarda due fronti distinti ma spesso sovrapposti nelle stesse aziende: (a) i nuovi divieti su nudifier tool e CSAM sintetico; (b) l'obbligo di watermarking tecnico dei contenuti generati dall'IA.

- **Aggiornare i contratti con i fornitori.**
  Inserire clausole aggiornate su watermarking, registrazione UE (anche per sistemi ritenuti esenti da alto rischio) e conformità alle nuove scadenze.

- **Verificare la sovrapposizione con normativa di prodotto.**
  Le aziende manifatturiere e i produttori di macchinari intelligenti dovrebbero rivalutare la classificazione dei propri sistemi alla luce della nuova definizione di "componente di sicurezza", per evitare adempimenti duplicati non più necessari.

- **Valutare l'integrazione FRIA/DPIA.**
  Le aziende che hanno già una struttura di data protection impact assessment matura possono pianificare l'assorbimento della FRIA, riducendo duplicazioni documentali quando saranno disponibili gli strumenti della Commissione.

- **Monitorare le comunicazioni ufficiali.**
  In particolare le decisioni della Commissione europea sulla disponibilità di norme armonizzate (che potrebbero anticipare le scadenze 2027/2028) e la pubblicazione in Gazzetta Ufficiale UE del regolamento di modifica, da cui decorre il termine di 3 giorni per l'entrata in vigore.

*Le informazioni contenute in questo capitolo riflettono lo stato della normativa al 3 luglio 2026, sulla base del testo approvato da Parlamento europeo e Consiglio UE. Trattandosi di una materia in rapida evoluzione, si raccomanda di verificare eventuali aggiornamenti successivi alla pubblicazione in Gazzetta Ufficiale dell'Unione Europea e i futuri atti di esecuzione e le linee guida della Commissione, prima di assumere decisioni vincolanti in materia di compliance.*

# La legge italiana 132/2025 sull'Intelligenza Artificiale

*Capitolo aggiunto in sede di aggiornamento - Luglio 2026*

## 1. Cos'è e come si colloca rispetto all'AI Act

La Legge 23 settembre 2025, n. 132 "Disposizioni e deleghe al Governo in materia di intelligenza artificiale" (pubblicata in Gazzetta Ufficiale n. 223 del 25 settembre 2025) è la normativa organica con cui l'Italia ha integrato, a livello nazionale, il Regolamento (UE) 2024/1689. Non si tratta di una disciplina alternativa all'AI Act - che resta direttamente applicabile in quanto regolamento europeo - ma di un layer normativo aggiuntivo che l'Italia ha adottato per disciplinare materie di competenza nazionale (sanità, pubblica amministrazione, giustizia, lavoro, professioni, profili penali e di responsabilità civile) in coerenza con l'approccio antropocentrico dell'AI Act.
La legge è entrata in vigore il 10 ottobre 2025. Si articola in sei capi e 28 articoli:

- Capo I - Principi e finalità: centralità della persona, approccio antropocentrico, principi di trasparenza, proporzionalità, robustezza, accuratezza, non discriminazione e protezione dei dati personali.

- Capo II - Disposizioni di settore: sanità (artt. 7 e 10), trattamento dei dati personali (art. 9), lavoro (artt. 1112), professioni intellettuali (art. 13), pubblica amministrazione (art. 14), attività giudiziaria (art. 15), cybersicurezza nazionale (art. 18).

- Capo III - Investimenti e promozione: fondi per l'ecosistema IA nazionale (art. 23), misure per giovani e sport (art. 22), sperimentazione presso il Ministero degli affari esteri (art. 21).

- Capo IV - Diritto d'autore: tutela estesa alle opere create con l'ausilio dell'IA, purché risultato del lavoro intellettuale dell'autore (nuovo art. 70-septies l. 633/1941).

- Capo V - Disposizioni penali: nuove fattispecie di reato legate a deepfake e usi illeciti dell'IA.

- Capo VI - Deleghe al Governo (art. 24) per l'adozione dei decreti legislativi attuativi, e disciplina organica su dati/algoritmi per l'addestramento (art. 16).

# La legge italiana 132/2025 sull'Intelligenza Artificiale

*Punto chiave per la compliance aziendale: la Legge 132/2025 non è "auto-applicativa". Gran parte delle sue disposizioni più operative (Autorità nazionale per l'IA, Registro nazionale degli algoritmi, elenco aggiornato dei sistemi high-risk, regime di responsabilità per danni da IA) richiede ancora decreti attuativi, molti dei quali sono in corso di elaborazione.*

## 2. Le disposizioni già operative rilevanti per le aziende

**2.1 Professioni intellettuali (art. 13)**
Per i professionisti (avvocati, commercialisti, ingegneri, consulenti, architetti, medici, e - per quanto qui rileva - anche per una società di compliance come la nostra) l'art. 13 stabilisce che l'uso dell'IA è consentito solo per attività strumentali e di supporto, con prevalenza del lavoro intellettuale umano nella prestazione.
È inoltre previsto un obbligo di trasparenza verso il cliente: il professionista deve comunicare in modo chiaro, semplice ed esaustivo se e in che misura ha utilizzato sistemi di IA nello svolgimento dell'incarico. La responsabilità della prestazione resta sempre in capo al professionista, non si trasferisce allo strumento.

- Implicazione operativa: chi eroga servizi professionali (legali, di consulenza, contabili) dovrebbe predisporre una informativa standard ex art. 13 da inserire in lettere di incarico e contratti, e verificare che i propri codici deontologici di categoria si siano aggiornati di conseguenza.

**2.2 Lavoro (artt. 11-12)**
Prima dell'utilizzo di sistemi di IA che incidono su decisioni relative ai lavoratori, il datore di lavoro deve adempiere agli obblighi informativi previsti dalla normativa vigente.
Il lavoratore ha diritto, su richiesta e con l'intervento di una persona fisica, a una motivazione intelligibile della decisione che lo riguarda, che indichi l'eventuale incidenza del sistema di IA sul processo decisionale e i principali parametri considerati.
È fatto salvo il diritto di accesso ai dati. Il licenziamento intimato in violazione del divieto di decisione esclusivamente automatizzata è nullo.

- Implicazione operativa: le aziende che usano sistemi di IA in ambito HR (screening, valutazione performance, decisioni su turni o incarichi) devono verificare la presenza di un adeguato processo di informativa preventiva e di un canale per la richiesta di intervento umano, distinto e complementare rispetto agli obblighi di trasparenza già previsti dall'AI Act per i sistemi high-risk o a rischio limitato.

**2.3 Diritto d'autore (Capo IV)**
La tutela autorale viene estesa alle opere dell'ingegno umano "anche laddove create con l'ausilio di strumenti di intelligenza artificiale, purché costituenti risultato del lavoro intellettuale dell'autore". È un chiarimento rilevante per i reparti marketing, comunicazione e R&D che producono contenuti con il supporto di strumenti generativi: la componente di creatività e scelta umana resta il presupposto per la tutela.

## 3. Lo stato dei decreti attuativi (aggiornamento a luglio 2026)

La legge delega il Governo ad adottare, entro 12 mesi dall'entrata in vigore - quindi entro il 10 ottobre 2026 - i decreti legislativi di adeguamento all'AI Act e di disciplina degli usi illeciti dell'IA (art. 24), oltre a una disciplina organica su dati e algoritmi per l'addestramento (art. 16).

- 10 giugno 2026 - il Consiglio dei Ministri (riunione n. 117/177) ha esaminato e approvato in via preliminare un primo pacchetto di decreti attuativi, tra cui uno schema di decreto legislativo che disciplina i poteri delle Autorità nazionali per l'IA e l'uso dell'IA in formazione, professioni, lavoro, sanità e pubblica amministrazione.

- Il pacchetto include disposizioni sulla formazione del personale della giustizia (articolata su tre piani: tecnico, giuridico, organizzativo/valoriale) e sugli obblighi informativi e di motivazione intelligibile per i lavoratori.

- Gli ordini professionali dovranno adeguare i propri regolamenti deontologici entro sei mesi dall'adozione dei decreti, con percorsi formativi obbligatori su tre piani: tecnico, giuridico, deontologico.

- Restano ancora da adottare, alla data di redazione di questo capitolo: il decreto legislativo sulla responsabilità civile e penale per usi illeciti dell'IA (delega più delicata, che dovrà disciplinare rimozione di contenuti illeciti, nuove fattispecie di reato per omessa adozione di misure di sicurezza, e uso dell'IA nelle indagini preliminari); il decreto sul trattamento dei dati sanitari mediante IA, il cui termine di delega (7 febbraio 2026) risulta già scaduto senza adozione; il decreto istitutivo del Registro nazionale degli algoritmi; il decreto istitutivo dell'Autorità nazionale per l'intelligenza artificiale.

*I decreti approvati il 10 giugno 2026 sono ancora all'esame preliminare: devono passare al vaglio delle Commissioni*

## La legge italiana 132/2025 sull'Intelligenza Artificiale

*parlamentari, della Conferenza delle Regioni e delle Authority competenti (incluso il Garante Privacy) prima dell'adozione definitiva. Il quadro è quindi ancora in evoluzione e alcuni contenuti potrebbero cambiare rispetto agli schemi attualmente circolati.*

### 4. Cosa manca ancora - aree di incertezza applicativa

Diverse disposizioni della Legge 132/2025 richiedono provvedimenti attuativi non ancora adottati:

- il Registro nazionale degli algoritmi sarà definito con decreto del Presidente del Consiglio dei ministri, su proposta dell'Agenzia per l'Italia Digitale (AgID);
- l'Autorità nazionale per l'intelligenza artificiale sarà istituita con decreto legislativo - a oggi manca ancora un'autorità di vigilanza nazionale dedicata e unificata;
- i percorsi formativi per dipendenti pubblici e professionisti saranno definiti con decreto interministeriale (Istruzione, Università, Lavoro);
  l'elenco nazionale dei sistemi di IA "ad alto rischio" sarà aggiornato periodicamente con decreto ministeriale, in coordinamento con l'AI Act europeo;
- le modalità di accertamento della responsabilità civile per danni causati da IA saranno oggetto di un decreto legislativo dedicato, in raccordo con il Codice civile e penale;
- sanzioni e procedure per contrastare la diffusione di contenuti manipolati (deepfake) saranno definite con regolamento attuativo.

Fino all'adozione di questi provvedimenti, le aziende operano in un contesto di incertezza applicativa su questi specifici punti, pur essendo già vincolate ai principi generali e alle disposizioni di settore già in vigore (artt. 7-18).

## 5. Tabella di sintesi - cosa fare già oggi

| Area | Azione consigliata |
|---|---|
| Servizi professionali erogati dall'azienda | Predisporre un'informativa standard ex art. 13 da inserire in lettere di incarico e contratti quando si utilizzano strumenti di IA nell'erogazione del servizio. |
| HR e gestione del personale | Verificare che i sistemi di IA usati su decisioni relative ai lavoratori prevedano informativa preventiva, motivazione intelligibile su richiesta e possibilità di intervento umano. |
| Marketing, comunicazione, R&D | Documentare l'apporto creativo umano nei contenuti prodotti con IA generativa, ai fini della tutela autorale. |
| Governance e monitoraggio normativo | Monitorare l'adozione dei decreti attuativi in vista della scadenza del 10 ottobre 2026, in particolare su responsabilità civile/penale e Autorità nazionale per l'IA. |
| Settori regolati (sanità, giustizia, PA) | Se applicabile, seguire le disposizioni di settore già in vigore (artt. 7, 10, 14, 15) e prepararsi ai decreti attuativi settoriali in corso di approvazione. |

*Le informazioni contenute in questo capitolo riflettono lo stato della normativa al 3 luglio 2026. La Legge 132/2025 è attualmente nella fase più delicata della sua attuazione, con numerosi decreti ancora in corso di elaborazione o approvazione parlamentare: si raccomanda un monitoraggio costante, in particolare in vista della scadenza del 10 ottobre 2026 per le deleghe principali, e di verificare gli aggiornamenti su questo tema anche indipendentemente dalle scadenze del Digital Omnibus europeo, trattandosi di percorsi normativi paralleli e distinti.*

# Conclusione: riepilogo operativo sull'AI Act

Questa guida è stata redatta con l'obiettivo di fornire tutti gli strumenti pratici per comprendere, valutare e implementare la compliance all'AI Act, nella sua versione aggiornata a seguito del Digital Omnibus. Di seguito, un riepilogo dei punti principali e della strada da intraprendere.

### Obiettivi dell'AI Act

- Protezione dei diritti fondamentali dei cittadini europei.
- Gestione dei rischi legati ai sistemi AI in azienda.
- Promozione di innovazione sicura e responsabile.
- Definizione di classi di rischio e obblighi proporzionati: Inaccettabile, High-Risk, Limited-Risk, MinimalRisk.

### Classificazione dei rischi (aggiornata)

- Inaccettabile: vietati già oggi (social scoring pubblico, sorveglianza subliminale) e, dal 2 dicembre 2026, anche nudifier tool e materiale pedopornografico sintetico.
- High-Risk: obblighi completi (AIA/FRIA, registri, supervisione umana, audit, contratti, sicurezza), applicabili dal 2 dicembre 2027 (sistemi autonomi) o dal 2 agosto 2028 (componenti di sicurezza), salvo anticipazione della Commissione.
- Limited-Risk: obblighi di trasparenza e disclosure verso utenti, con watermarking tecnico dei contenuti sintetici dal 2 dicembre 2026.
- Minimal-Risk: nessun obbligo specifico, applicazione di buone pratiche.

### Obblighi principali per i sistemi AI

- Creazione di registro interno AI.
- Documentazione tecnica e log operativi.
- Valutazioni di impatto (AIA/FRIA, eventualmente assorbita nella DPIA) per High-Risk.
- Supervisione umana e procedure operative.
- Contratti conformi con fornitori (clausole di compliance, audit, SLA, gestione vulnerabilità, watermarking, registrazione UE).
- Trasparenza e formazione dei dipendenti (AI Literacy).
- Meccanismi di gestione degli incidenti.
- Per le aziende italiane: verifica di conformità anche alla Legge 132/2025 (informativa ex art. 13 per servizi professionali, obblighi verso i lavoratori ex artt. 11-12), oltre all'AI Act.

# Conclusione: riepilogo operativo sull'AI Act

**Roadmap di adeguamento**

- Preparazione e governance: costituire team AI compliance, definire obiettivi e policy interne.
- Inventario e classificazione dei sistemi AI: mappatura dei sistemi, categorizzazione dei rischi, richiesta documentazione ai fornitori.
- Valutazioni e obblighi di compliance: AIA/FRIA, human oversight, aggiornamento registro e contratti.
- Implementazione operativa: procedure interne, formazione, integrazione nei processi aziendali.
- Monitoraggio e miglioramento continuo: audit, aggiornamento log e metriche, revisione policy e formazione.
- Prossime scadenze normative: 2 dicembre 2026 (divieti nudifier/ CSAM e watermarking); 2 agosto 2027 (sandbox); 2 dicembre 2027 e 2 agosto 2028 (obblighi high-risk).

**Conclusione**

Seguendo questa guida aggiornata, l'azienda può:

- Comprendere chiaramente quali sistemi AI sono soggetti a vincoli e quali rischi comportano, alla luce delle nuove scadenze.
- Pianificare un percorso di adeguamento strutturato, tracciabile e correttamente scandito nel tempo fino al 2028.
- Integrare governance, formazione, contratti e procedure operative per garantire compliance e ridurre rischi.
- Prepararsi a future ispezioni o audit - anche da parte del rafforzato AI Office europeo - e mantenere un approccio proattivo nell'uso dell'AI.

In sintesi, questa guida non è solo un manuale di compliance, ma uno strumento pratico e operativo per implementare un'AI responsabile, sicura e conforme alla normativa europea, aggiornato alle più recenti evoluzioni del quadro regolatorio, con lo scopo di lasciarvi consapevoli della strada da percorrere.


Largo Umberto Boccioni 1
21040 Origgio VA
T. +39 02 96515401

Altre sedi
Milano - Pesaro - Udine

avvera.it - info@avvera.it