GUIDA RAPIDA

AI Act: in quale quadrante si colloca la vostra azienda, e che cosa comporta

Regolamento (UE) 2024/1689 in sei pagine: le due variabili che determinano gli obblighi, il percorso per classificare ogni uso, le azioni da compiere.

2 ruoli × 4 livelli
Gli obblighi dipendono da chi siete e da come usate il sistema, non dalla tecnologia

Già in vigore
Alfabetizzazione del personale e pratiche vietate dal 2 febbraio 2025; trasparenza dal 2 agosto 2026

2 dic 2027
Applicazione degli obblighi sull'alto rischio (Allegato III), rinviata dall'Omnibus digitale

fino al 7%
del fatturato mondiale annuo, o 35 milioni di euro se superiore, per le pratiche vietate

01 L'AI Act in sessanta secondi

Che cos'è. Il primo regolamento organico sull'intelligenza artificiale, direttamente applicabile in tutta l'Unione senza recepimento. In vigore dal 1° agosto 2024; modificato dal Regolamento (UE) 2026/1744, l'*Omnibus digitale sull'IA* (*Digital Omnibus on AI*), in vigore dal 27 luglio 2026.

A chi si applica. A chiunque sviluppi, immetta sul mercato o utilizzi sistemi di IA nell'Unione per fini professionali. Nessuna soglia dimensionale: riguarda anche le PMI (con alcune semplificazioni) e anche chi usa soltanto strumenti di terzi.

Come ragiona. Non regola la tecnologia, regola l'uso. Gli obblighi discendono da due variabili: il **ruolo** dell'azienda — *deployer*, cioè utilizzatore, se usa un sistema di terzi; *fornitore* (*provider*) se lo sviluppa e lo mette in servizio — e il **livello di rischio** dell'impiego concreto. Stesso strumento, usi diversi, obblighi diversi.

Che cosa vale già. L'obbligo di alfabetizzazione del personale (art. 4) e i divieti (art. 5), dal 2 febbraio 2025. Gli obblighi di trasparenza (art. 50), dal 2 agosto 2026.

Che cosa arriva. Gli obblighi sui sistemi ad alto rischio: Allegato III dal 2 dicembre 2027, Allegato I dal 2 agosto 2028. Chi mette in servizio un sistema dopo quelle date li rispetta da subito; i sistemi già in servizio restano fuori finché non subiscono «modifiche significative della progettazione» (art. 111, par. 2) — nozione non definita, che un aggiornamento del fornitore può integrare: non è una base su cui pianificare.

02 Tre convinzioni sbagliate

«Usiamo solo un assistente di terzi, non ci riguarda.»
Vi riguarda. Chi utilizza un sistema di IA per fini professionali è *deployer*, e già oggi deve adottare misure per l'alfabetizzazione del personale (art. 4) e rispettare i divieti. Il fornitore dello strumento non adempie al posto vostro.

«Lo strumento è conforme, quindi siamo a posto.»
Si classifica l'uso, non lo strumento. Lo stesso modello è a rischio minimo se aiuta a scrivere codice e ad alto rischio se filtra candidature. La conformità del prodotto non copre l'impiego che ne fate.

«Lo abbiamo sviluppato per uso interno, non siamo fornitori.»
Lo siete. La messa in servizio comprende espressamente l'uso proprio (art. 3, punto 11). Sviluppare un sistema di IA e usarlo in casa rende fornitori — con obblighi che restano leggeri solo finché il sistema non è ad alto rischio.

03 Come usare questa guida

1 **Determinate il ruolo**
Deployer o fornitore? Quattro domande in sequenza, con i casi tipici già risolti.
Pagina 3 — Passo 1

2 **Determinate il livello di rischio**
Dal più grave al meno grave, fermandosi alla prima risposta affermativa. Con gli elenchi di ciò che cade dove.
Pagine 3 e 4 — Passo 2

3 **Leggete la vostra cella**
Obblighi e azioni concrete per ciascuna delle otto celle, più quelli che valgono sempre.
Pagina 5 — poi date, sanzioni e primi trenta giorni a pagina 6

Il punto per la direzione. Per la quasi totalità delle aziende che usano strumenti di terzi, il costo di conformità è oggi la formazione del personale e una policy interna. Gli adempimenti costosi riguardano i sistemi ad alto rischio, che si costruiscono o si adottano per scelta.

04 Le due variabili

Deployer (utilizzatore) — chi usa

Chi utilizza un sistema di IA **sotto la propria autorità** nell'esercizio di un'attività professionale (art. 3, punto 4). Il testo italiano del Regolamento lascia il termine in inglese; in questa guida vale «utilizzatore professionale». È il ruolo di chiunque usi strumenti forniti da terzi.

Fornitore (provider) — chi sviluppa e mette in servizio

Chi sviluppa un sistema di IA, o lo fa sviluppare, e lo immette sul mercato **o lo mette in servizio** con il proprio nome o marchio, a titolo oneroso o gratuito (art. 3, punto 3). La messa in servizio comprende l'uso proprio (punto 11).

I QUATTRO LIVELLI DI RISCHIO

Inaccettabile
Pratiche vietate dall'art. 5. Nessuna eccezione rilevante per un'impresa.

Elevato
Nel Regolamento: «alto rischio». Sistemi dell'Allegato III o componenti di sicurezza di prodotti (Allegato I). Il pacchetto pesante.

Di trasparenza
Sistemi che interagiscono con persone o generano contenuti (art. 50). Obblighi di informazione.

Minimo o nullo
Categoria residuale: tutto il resto. Nessun requisito di prodotto.

05 La matrice

Ogni cella ha un codice, richiamato a pagina 5 con obblighi e azioni.

Livello di rischio	Come DEPLOYER — usate un sistema di terzi	Come FORNITORE — sviluppate e mettete in servizio
Minimo o nullo categoria residuale	**A1** Solo obblighi trasversali: formazione del personale e divieti. Nessun requisito di prodotto. È qui che si colloca la grande maggioranza degli usi aziendali attuali.	**A2** Solo obblighi trasversali. Se il sistema tocca un ambito dell'Allegato III e invocate l'eccezione dell'art. 6, par. 3: valutazione documentata e registrazione nella banca dati UE.
Di trasparenza art. 50	**B1** Dichiarare i deep fake e i testi generati pubblicati su questioni di interesse pubblico; informare le persone esposte a riconoscimento delle emozioni o categorizzazione biometrica.	**B2** Progettare il sistema perché l'utente sappia di interagire con un'IA; marcare i contenuti generati in formato leggibile da macchina.
Elevato art. 6, Allegati I e III	**C1** Art. 26: sorveglianza umana qualificata, log per almeno sei mesi, informativa preventiva ai lavoratori, monitoraggio, informazione alle persone soggette a decisione.	**C2** L'intero Capo III: gestione del rischio, governo dei dati, documentazione tecnica, valutazione di conformità, marcatura CE, registrazione nella banca dati UE, monitoraggio post-commercializzazione.
Inaccettabile art. 5	**D1** Vietato. Cessazione immediata dell'uso.	**D2** Vietato. Cessazione e ritiro del sistema.

Quattro regole di lettura. 1. Si classifica l'uso, non lo strumento: un sistema con più usi va classificato per ciascuno. **2.** Il livello si determina scendendo dal più grave e fermandosi alla prima risposta affermativa — non si sceglie quello più comodo. **3.** Formazione del personale (art. 4) e divieti (art. 5) valgono in ogni cella, anche in A1: «nessun requisito di prodotto» non significa nessun obbligo. **4.** Le colonne non si escludono e gli obblighi si sommano: chi sviluppa e usa in casa sta in entrambe (A1+A2, o C1+C2); un sistema ad alto rischio che dialoga con persone rispetta anche l'art. 50.

Altri ruoli. Chi sviluppa o addestra un *modello di IA per finalità generali* ha obblighi propri (artt. 53–55): non riguarda chi usa o integra modelli altrui, salvo un addestramento aggiuntivo significativo. Chi importa da fuori UE o distribuisce prodotti con IA integrata ad alto rischio ha obblighi di verifica propri (artt. 23–24).

Se siete una PMI. Nessuna esenzione, ma semplificazioni: documentazione tecnica dell'alto rischio in forma semplificata (art. 11); sistema di gestione della qualità proporzionato alla dimensione, con elementi semplificati per chi non ha imprese collegate (artt. 17, 63); sanzioni al **minore** tra percentuale e importo fisso, anziché al maggiore (art. 99, par. 6); accesso prioritario e gratuito ai sandbox regolamentari, formazione dedicata, canali con le autorità, tariffe ridotte per la valutazione di conformità (artt. 57–58, 62). L'Omnibus estende le semplificazioni alle **piccole imprese a media capitalizzazione** (secondo la definizione della Commissione europea), con le sanzioni ridotte limitate alle fasce del 3% e dell'1%. **Attenzione al criterio:** è PMI chi ha meno di 250 dipendenti *e* fatturato non superiore a 50 M€ o bilancio non superiore a 43 M€ (Racc. 2003/361/CE). Un'azienda con pochi dipendenti ma fatturato elevato non è PMI: per lei vale il maggiore dei due importi.

06 Il percorso di classificazione

Due passi, sempre in questo ordine. In ciascuno, la prima risposta affermativa chiude il passo.

PASSO 1 — QUAL È IL VOSTRO RUOLO?

R1 **Il risultato del lavoro è un sistema di IA — incorpora un modello e ne usa gli output per produrre previsioni, contenuti, raccomandazioni o decisioni?**

SÌ → prosegui con R2

NO ↓ Non c'è nulla da classificare. Usare l'IA per scrivere software ordinario non produce un sistema di IA: siete deployer dello strumento usato, già classificato a sé.

R2 **L'avete sviluppato, o fatto sviluppare su vostre specifiche, e lo mettete in servizio con il vostro nome — anche solo per uso proprio?**

SÌ → FORNITORE (colonna 2) | NO ↓ prosegui con R3

R3 **È di terzi, ma (a) lo mettete in servizio con il vostro nome o marchio (art. 3, punto 3), oppure (b) è ad alto rischio e vi apponete il marchio o lo modificate sostanzialmente, o ne cambiate la finalità rendendolo ad alto rischio (art. 25, par. 1)?**

SÌ → FORNITORE del sistema modificato | NO ↓ prosegui con R4

R4 **Lo utilizzate sotto la vostra autorità nell'esercizio di un'attività professionale?**

SÌ → DEPLOYER (colonna 1) | NO ↓ Uso personale non professionale: fuori dal Regolamento.

CASI TIPICI

Caso	Ruolo	Cella
Assistente di codice di terzi usato dall'IT	Deployer	**A1**
Script interno che interroga un modello linguistico per classificare i ticket	Fornitore (e deployer)	**A2 + A1**
Gestionale con funzione di IA integrata dal produttore	Deployer; il fornitore è il produttore	**A1** o **C1** secondo la funzione
Chatbot di terzi personalizzato e offerto ai clienti a proprio nome	Fornitore	**B2**
Assistente di terzi usato per filtrare i curriculum	Deployer	**C1**

PASSO 2 — QUAL È IL LIVELLO DI RISCHIO?

L1 **L'uso rientra in una pratica vietata dall'art. 5? (elenco a pagina 4)**

SÌ → INACCETTABILE (riga D) | NO ↓ prosegui con L2

L2 **È un componente di sicurezza di un prodotto regolato (Allegato I), oppure è destinato a un ambito dell'Allegato III — e non ricade nell'eccezione dell'art. 6, par. 3?**

SÌ → ELEVATO (riga C) | NO ↓ prosegui con L3

L3 **Il sistema parla con le persone o produce contenuti?**

deployer Se usate uno strumento di terzi, l'obbligo è **dichiarare**, e scatta solo per un **deep fake** — immagine, audio o video realistico di persone, luoghi o eventi reali — o per un **testo su questioni di interesse pubblico** non rivisto da un umano, o se esponete persone a riconoscimento delle emozioni. Illustrazioni generiche, riassunti e testi interni: nessun obbligo. Il watermark non spetta a voi.

fornitore Se fornite il sistema, dovete progettarlo perché l'utente sappia di interagire con un'IA e perché i contenuti generati siano **marcati** in modo leggibile da macchina.

SÌ → DI TRASPARENZA (riga B) | NO ↓ prosegui con L4

L4 **Nessuna delle precedenti → MINIMO O NULLO (riga A).** Categoria residuale: vi rientra ciò che non è vietato, non è ad alto rischio e non ricade nell'art. 50.

L'eccezione dell'art. 6, par. 3. Un sistema in un ambito dell'Allegato III non è ad alto rischio se svolge un compito procedurale ristretto, migliora un'attività umana già completata, rileva schemi decisionali senza sostituire la valutazione umana, o svolge un compito preparatorio. **Non si applica mai se il sistema profila persone fisiche.** Chi la invoca documenta la valutazione prima della messa in servizio (par. 4) e registra il sistema nella banca dati UE (art. 49, par. 2).

Il salto che nessuno firma. Si cambia cella senza accorgersene: un prototipo interno che va in produzione, un'automazione estesa a un processo che riguarda persone, un contenuto generato pubblicato senza revisione. Per questo nessun nuovo uso dovrebbe partire senza classificazione preventiva scritta.

Un percorso completo. Un'azienda vuole usare un assistente di terzi per riassumere e ordinare i curriculum ricevuti. **Passo 1:** R1 sì; R2 no; R3 no — purché le condizioni d'uso del fornitore non escludano l'impiego per la selezione del personale: verificatelo sempre, se lo escludono la cella cambia; R4 sì → **deployer**. **Passo 2:** L1 no; L2 sì — analisi e filtro delle candidature, Allegato III, ambito occupazione; l'eccezione non si applica perché il sistema profila persone → **rischio elevato**, cella **C1**. **Da oggi:** GDPR (DPIA, art. 22) e informativa a lavoratori e rappresentanze sindacali sui sistemi decisionali o di monitoraggio integralmente automatizzati (d.lgs. 152/1997, art. 1-bis). **Dal 2 dicembre 2027**, se messo in servizio o modificato in modo significativo dopo quella data: art. 26. Lo stesso assistente usato per riassumere documentazione tecnica interna sarebbe in **A1**: stesso strumento, cella diversa.

07 Dove cadono i casi concreti

L1 · PRATICHE VIETATE (ART. 5)

Riconoscimento delle emozioni da dati biometrici (volto, voce) sul luogo di lavoro e nell'istruzione, salvo motivi medici o di sicurezza delle persone. Copre selezione e periodo di prova: analisi delle espressioni dei dipendenti in videosorveglianza, del loro tono di voce nelle chiamate, dello stress nei colloqui. Sui clienti non è vietato, ma è alto rischio e richiede l'informativa.

Categorizzazione biometrica per dedurre razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita o orientamento sessuale.

Punteggio sociale: valutare o classificare persone nel tempo in base al comportamento sociale o a caratteristiche personali, con trattamenti sfavorevoli in contesti non correlati oppure ingiustificati o sproporzionati.

Tecniche subliminali o manipolative che distorcono il comportamento causando, o potendo ragionevolmente causare, un danno significativo; **sfruttamento di vulnerabilità** dovute a età, disabilità, condizione sociale o economica.

Raccolta non mirata di immagini facciali da internet o videosorveglianza per banche dati di riconoscimento.

Previsione del rischio di reato basata solo su profilazione o tratti della personalità; **identificazione biometrica remota in tempo reale** in spazi pubblici a fini di contrasto.

Dal 2 dicembre 2026: sistemi che generano contenuti intimi o sessualmente espliciti di persone riconoscibili senza consenso, o materiale di abuso sessuale su minori. Per chi sviluppa sistemi generativi: vietato se la generazione è la finalità o un risultato prevedibile in assenza di misure tecniche di sicurezza; per chi li usa, se li usa a quel fine.

L2 · ALTO RISCHIO: GLI AMBITI DELL'ALLEGATO III

Occupazione e gestione dei lavoratori. Selezione dei candidati, analisi e filtro delle candidature, valutazione dei colloqui, decisioni su promozione o cessazione, assegnazione di compiti in base a comportamento o tratti personali, monitoraggio e valutazione delle prestazioni. L'ambito in cui le aziende entrano più spesso senza rendersene conto.

Accesso a servizi essenziali. Affidabilità creditizia di persone fisiche; prezzo di assicurazioni vita e salute; prestazioni pubbliche; triage delle emergenze. Esclusi i sistemi per individuare frodi finanziarie.

Biometria. Identificazione remota, categorizzazione secondo attributi sensibili, riconoscimento delle emozioni ove non vietato.

Istruzione e formazione professionale. Ammissione, valutazione dell'apprendimento, controllo durante gli esami.

Infrastrutture critiche. Componenti di sicurezza di reti energetiche, idriche, digitali e di trasporto.

Contrasto, migrazione, giustizia e processi democratici: ambiti riservati in prevalenza al settore pubblico.

Allegato I. Sezione A: prodotti con valutazione di conformità di terza parte — dispositivi medici, ascensori, giocattoli, apparecchiature radio e a pressione, DPI — applicazione diretta dal 2 agosto 2028. Macchine, veicoli, aeronautica e ferrovie stanno in sezione B: l'AI Act non si applica direttamente, i requisiti arriveranno nella normativa di prodotto. Dopo l'Omnibus, l'IA per controllo qualità, ottimizzazione o assistenza all'operatore non è «componente di sicurezza» se il suo guasto non mette a rischio salute e sicurezza (art. 6, par. 1-bis e 1-ter).

L3 · TRASPARENZA (ART. 50): CHE COSA LA ATTIVA, E PER CHI

fornitore	Sistemi destinati a **interagire direttamente con persone** — assistenti, chatbot, agenti conversazionali (par. 1).
fornitore	Sistemi che **generano contenuti sintetici**: testo, immagini, audio, video — obbligo di marcatura (par. 2).
deployer	Persone esposte a **riconoscimento delle emozioni o categorizzazione biometrica**, nei casi non vietati (par. 3).
deployer	**Deep fake** generati o manipolati; **testi generati e pubblicati** per informare il pubblico su questioni di interesse pubblico, se non rivisti da un umano con responsabilità editoriale (par. 4).

Il watermark è di chi fornisce; la dichiarazione è di chi usa, e solo per deep fake e testi di interesse pubblico. Illustrazioni generiche, riassunti e testi interni non attivano l'art. 50 per chi li usa: restano in A1.

L4 · RISCHIO MINIMO: ESEMPI

Assistenza alla scrittura di codice, documentazione e testi interni; analisi di log; riassunti e traduzioni a uso interno con revisione umana.

Automazioni su processi che non riguardano persone; filtri antispam; sistemi di raccomandazione interni senza effetti su persone; ottimizzazione di magazzino o produzione.

Restano comunque: formazione del personale, rispetto dei divieti, GDPR se sono trattati dati personali.

08 Obblighi e azioni per ciascuna cella

Livello	Come DEPLOYER	Come FORNITORE
Minimo o nullo	**A1** • Formare gli utilizzatori (art. 4) e adottare una policy d'uso. • Verificare le condizioni del fornitore: esclusione dell'addestramento sui vostri dati, accordo sul trattamento, sede di elaborazione, usi esclusi. • Registro interno con la motivazione della classificazione; rivalutare a ogni cambio di finalità o di dati. Verifica umana dei risultati, documentata.	**A2** • Documentare la classificazione: è la prova più economica da produrre. Se invocate l'eccezione dell'art. 6, par. 3, è un obbligo, con registrazione nella banca dati UE (art. 49, par. 2). • Descrivere finalità prevista, dati in ingresso e usi esclusi in una scheda tecnica interna. • Procedura per sospendere il sistema e raccogliere le segnalazioni; rivalutare a ogni estensione d'uso. Codici di condotta volontari (art. 95).
Di trasparenza	**B1** • Deep fake: dichiarare che il contenuto è generato o manipolato; nelle opere manifestamente artistiche o satiriche basta una segnalazione adeguata (par. 4). • Testi generati pubblicati su questioni di interesse pubblico: dichiararlo, salvo revisione umana con responsabilità editoriale (par. 4). • Informare le persone esposte a riconoscimento delle emozioni o categorizzazione biometrica (par. 3). • Nessun contenuto verso l'esterno senza revisione. La marcatura è obbligo del fornitore: verificate che la applichi.	**B2** • Progettare il sistema perché la persona sappia di interagire con un'IA, salvo evidenza (par. 1). • Marcare i contenuti generati in formato leggibile da macchina, con soluzioni efficaci, interoperabili, robuste e affidabili (par. 2). • Inserire l'avviso all'utente nel progetto, non dopo; verificare che la marcatura sopravviva alle vostre elaborazioni. • Sistemi immessi sul mercato prima del 2 agosto 2026: marcatura entro il 2 dicembre 2026; per quelli successivi, da subito.
Elevato dal 2 dic 2027 (All. III) dal 2 ago 2028 (All. I)	**C1** art. 26 • Usare il sistema secondo le istruzioni del fornitore; dati di input pertinenti e rappresentativi; monitoraggio, segnalazione e sospensione se emerge un rischio; notifica immediata degli incidenti gravi. • Sorveglianza umana affidata a persone competenti, formate e con l'autorità per ignorare o ribaltare l'output. • Log conservati per almeno sei mesi, nella misura in cui sono sotto il vostro controllo: con strumenti in cloud va previsto nel contratto. • **Informare i lavoratori e i loro rappresentanti prima della messa in servizio** sul luogo di lavoro. • Informare le persone soggette a decisioni; garantire il diritto a una spiegazione (art. 86). • Valutazione d'impatto sui diritti fondamentali (art. 27) per enti pubblici, servizi pubblici, credito e assicurazioni. **Da oggi**, a prescindere dalle date: DPIA e informativa a lavoratori e rappresentanze sindacali (d.lgs. 152/1997, art. 1-bis).	**C2** Capo III • **Progettare secondo i requisiti** (artt. 9–15): gestione dei rischi, governo dei dati, documentazione tecnica, registrazione degli eventi, istruzioni per l'uso, sorveglianza umana, accuratezza e cibersicurezza. • **Sistema di gestione della qualità** e conservazione della documentazione per dieci anni (artt. 17–18); azioni correttive (20). • **Valutare la conformità, marcare CE, registrare** nella banca dati UE (artt. 43, 47–49). Per gli ambiti 2–8 dell'Allegato III è un'autovalutazione interna, senza organismo notificato; l'organismo serve solo per la biometria. • **Monitorare e segnalare** gli incidenti gravi (artt. 72–73). • **Catena del valore** (art. 25): accordi scritti con i sub-fornitori, anche di modelli, su informazioni e accesso tecnico; chi ha fornito un sistema poi reso ad alto rischio da altri coopera con il nuovo fornitore, salvo esclusione scritta. • **Prima di tutto:** chiedersi se il sistema vada davvero costruito internamente. Il costo di C2 è di un altro ordine di grandezza rispetto a C1.
Inaccettabile	**D1** • Cessare immediatamente l'uso; documentare data e misure adottate. • Verificare se i dati raccolti debbano essere cancellati ai sensi del GDPR.	**D2** • Cessare la messa in servizio, ritirare il sistema, informare i deployer a cui è stato fornito. • Conservare le evidenze della cessazione.

IN OGNI CELLA

Alfabetizzazione — art. 4

Misure volte a sostenere lo sviluppo dell'alfabetizzazione in materia di IA del personale, calibrate su conoscenze, esperienza e contesto d'uso. Nessun livello minimo, nessuna certificazione: conta poter dimostrare le misure adottate — presenze, materiali, esiti.

GDPR e diritto nazionale

Il GDPR si applica in parallelo: base giuridica, registro dei trattamenti, DPIA, art. 22 sulle decisioni automatizzate. In Italia si sommano l'informativa sui sistemi integralmente automatizzati (d.lgs. 152/1997, art. 1-bis) e la Legge 132/2025.

Finalità prevista e condizioni d'uso

La finalità dichiarata dal fornitore — istruzioni, condizioni, materiale promozionale — decide se il vostro uso è coperto. Un uso che il fornitore esclude può farvi diventare fornitori (art. 25, par. 1, lett. c). Leggere gli usi esclusi è il primo controllo.

09 Le date che contano

2 feb 2025
Art. 4 alfabetizzazione; art. 5 pratiche vietate

2 ago 2025
Obblighi GPAI; governance; sanzioni

2 ago 2026
Applicazione generale; art. 50 trasparenza

2 dic 2026
Marcatura per i sistemi già sul mercato; nuovi divieti art. 5

2 dic 2027
Alto rischio — Allegato III

2 ago 2028
Alto rischio — Allegato I, sezione A

Sistemi ad alto rischio già in servizio prima di quelle date: fuori dagli obblighi finché non subiscono «modifiche significative della progettazione» (art. 111, par. 2) — nozione non definita, che un riaddestramento o un aggiornamento di versione può integrare; quelli usati per conto di autorità pubbliche si adeguano comunque entro il 2 agosto 2030. Chi mette in servizio dopo le date rispetta gli obblighi da subito.

10 Le sanzioni

Violazione	Massimo (art. 99)
Pratiche vietate (art. 5)	**35 M€ o 7%** del fatturato mondiale annuo, se superiore
Obblighi di fornitori, deployer e trasparenza	**15 M€ o 3%**, se superiore
Informazioni inesatte alle autorità	**7,5 M€ o 1%**, se superiore

Per le PMI si applica il minore dei due importi; per le piccole imprese a media capitalizzazione solo nelle fasce del 3% e dell'1% (criteri e semplificazioni a pagina 2). L'art. 4 non ha una fascia propria nell'art. 99; le misure organizzative adottate pesano nella quantificazione di ogni altra sanzione (art. 99, par. 7).

CHI VIGILA, IN ITALIA

La Legge 132/2025 designa **AgID** (promozione, notifica e accreditamento degli organismi di valutazione) e **ACN** (vigilanza di mercato, ispezioni, sanzioni). Il Garante privacy resta competente sui trattamenti di dati personali. La legge richiama l'obbligo, già in vigore, di informare lavoratori e rappresentanze sindacali sui sistemi decisionali o di monitoraggio integralmente automatizzati, e impone ai professionisti di informare il cliente sull'uso di IA.

11 I primi trenta giorni

- [ ] **Censire** gli strumenti di IA già in uso, compresi quelli su account personali e le funzioni attive per impostazione predefinita nei programmi aziendali.
- [ ] **Classificare** ogni uso con il percorso di pagina 3 e annotare la cella, con la motivazione.
- [ ] **Aprire un registro** dei sistemi di IA: una riga per sistema, con ruolo, livello, dati trattati, referente, data di revisione.
- [ ] **Adottare una policy d'uso**: strumenti ammessi, informazioni che non si inseriscono mai, verifica umana, usi vietati, procedura per i nuovi casi d'uso.
- [ ] **Contrattualizzare** gli strumenti su piani aziendali che escludano l'uso dei dati per l'addestramento, con accordo sul trattamento; **leggere gli usi esclusi** dal fornitore.
- [ ] **Formare** il personale in modo proporzionato al ruolo e conservare le evidenze: con il rispetto dei divieti, è l'obbligo che riguarda già tutti.
- [ ] **Coinvolgere il DPO** prima dell'attivazione, non dopo: base giuridica, analisi di soglia, eventuale DPIA.
- [ ] **Fissare la regola**: nessun nuovo caso d'uso senza classificazione preventiva scritta. È la misura che impedisce di cambiare cella senza accorgersene.

12 Sei termini da conoscere

Sistema di IA
Sistema automatizzato che, con livelli variabili di autonomia, deduce dagli input come generare output — previsioni, contenuti, raccomandazioni, decisioni (art. 3, punto 1). Uno script deterministico non lo è; un programma che interroga un modello sì.

Finalità prevista
L'uso per cui il fornitore destina il sistema, come risulta da istruzioni, materiale promozionale e documentazione (punto 12). Decide la cella, e decide se un uso diverso vi rende fornitori.

Profilazione
Trattamento automatizzato di dati personali per valutare aspetti di una persona — rendimento, situazione economica, salute, preferenze, comportamento (GDPR, art. 4, punto 4). Se c'è, l'eccezione dell'art. 6, par. 3 è esclusa.

Componente di sicurezza
Parte di un prodotto la cui funzione è di sicurezza, o il cui guasto mette a rischio salute, sicurezza o beni (punto 14). Dopo l'Omnibus, non lo sono controllo qualità, ottimizzazione e assistenza all'operatore se il guasto non crea rischio.

Modifica sostanziale
Modifica non prevista nella valutazione di conformità iniziale che incide sulla conformità o sulla finalità prevista (punto 23). Apportarla a un sistema ad alto rischio altrui fa assumere il ruolo di fornitore.

Modello per finalità generali
Modello addestrato su larga scala, capace di un'ampia gamma di compiti e integrabile in sistemi diversi (punto 63). Chi lo sviluppa ha obblighi propri; chi lo integra non li ha, ma resta fornitore del sistema che ci costruisce sopra.

Questa guida ha finalità informative e non costituisce parere legale. Riferimenti: Regolamento (UE) 2024/1689 e Regolamento (UE) 2026/1744 su EUR-Lex; Legge 23 settembre 2025, n. 132; orientamenti della Commissione europea sulle pratiche vietate e sulla definizione di sistema di IA (febbraio 2025), sugli obblighi di trasparenza dell'art. 50 e Codice di buone pratiche sui contenuti generati (luglio 2026), bozza di orientamenti sulla classificazione dei sistemi ad alto rischio (maggio 2026). Denominazioni dei livelli di rischio secondo la Commissione europea. Versione 1.5 — settembre 2026. Corso gratuito collegato: «AI Act Formazione», tre video lezioni per chi usa l'IA al lavoro.