Yellow Tech

EDIZIONE AGOSTO 2026

GUIDA OPERATIVA · REGOLAMENTO (UE) 2024/1689

AI Act Compliance Checklist

51 punti di controllo per capire subito se la tua azienda è in regola

Dal 2 agosto 2026 l'AI Act è entrato nella fase di applicazione generale: le autorità di vigilanza sono operative e le sanzioni sono pienamente applicabili. Questa checklist, aggiornata al Digital Omnibus (Reg. UE 2026/1744), ti guida sezione per sezione tra gli obblighi già in vigore e quelli in arrivo nel 2027–2028.

✓ Aggiornata alle nuove scadenze del Digital Omnibus · agosto 2026

7%
del fatturato mondiale: la sanzione massima per le violazioni più gravi

51
punti di controllo organizzati in 8 aree di conformità

3
scadenze da presidiare tra oggi e agosto 2028

15min
il tempo necessario per una prima autovalutazione

IL QUADRO IN 3 MINUTI

Cosa è in vigore oggi (e cosa slitta al 2027–2028)

L'AI Act si applica per fasi. Il Digital Omnibus sull'IA (Reg. UE 2026/1744, in vigore dal 27 luglio 2026) ha rinviato gli obblighi sui sistemi ad alto rischio, ma ha lasciato ferma la data del 2 agosto 2026 per tutto il resto: trasparenza verso il pubblico, vigilanza nazionale e sanzioni. Tradotto: la fase in cui "c'è tempo" è finita.

VIOLAZIONE	SANZIONE MASSIMA	CHI RISCHIA
Pratiche di AI vietate (Art. 5)	**35 mln € / 7% fatturato**	Chiunque le impieghi: fornitori e utilizzatori
Violazione degli altri obblighi (es. trasparenza Art. 50)	**15 mln € / 3% fatturato**	Fornitori, deployer, importatori, distributori
Informazioni inesatte o fuorvianti alle autorità	**7,5 mln € / 1% fatturato**	Chiunque risponda a una richiesta di vigilanza

Per le PMI si applica l'importo inferiore tra soglia fissa e percentuale. Restano ferme, in parallelo, le sanzioni GDPR e le responsabilità civilistiche degli amministratori (art. 2086 c.c., assetti adeguati).

Chi vigila in Italia. La L. 132/2025 designa ACN come autorità di vigilanza del mercato, con poteri ispettivi e sanzionatori sui sistemi di AI, e AgID come autorità di notifica degli organismi di valutazione della conformità.

Come usare questa checklist

Per ogni punto, segna una delle tre caselle. Alla fine, conta i ✓ e vai alla pagina del punteggio.

✓

Fatto e documentato. Non basta "lo facciamo": deve esistere evidenza scritta che lo dimostri a un'autorità.

✗

Non fatto. Il punto non è presidiato o non è mai stato affrontato in azienda.

?

Non lo so. Attenzione: ai fini del rischio, un "non lo so" vale quanto un "no".

Più di tre "✗" o "?" in una singola sezione? È il segnale che serve una verifica strutturata. In 30 minuti di call gratuita mappiamo insieme le tue priorità reali.

Prenota una call → yellowtech.it/contattaci

2 feb 2025
Pratiche vietate (Art. 5) e alfabetizzazione AI (Art. 4)

2 ago 2025
Obblighi per i modelli GPAI, governance e quadro sanzionatorio

2 ago 2026
Applicazione generale: trasparenza (Art. 50), autorità di vigilanza operative, sanzioni applicabili

2 dic 2026
Applicazione piena dei divieti su deepfake intimi non consensuali e CSAM generato con AI, già introdotti dal 27 luglio 2026

2 ago 2027
Conformità dei modelli GPAI immessi sul mercato prima del 2 ago 2025

2 dic 2027
Obblighi alto rischio per i sistemi "stand-alone" (Allegato III)

2 ago 2028
Obblighi alto rischio per l'AI integrata in prodotti regolamentati (Allegato I)

Le fondamenta: sai quali AI usi e con quale ruolo?

1 Censimento e classificazione dei sistemi AI

DA FARE ORA

Artt. 3, 6, 25 · Allegato III · il punto di partenza obbligato di qualsiasi percorso di conformità

- ☐ ☐ ☐ Abbiamo un inventario aggiornato di tutti i sistemi e le funzionalità di AI in uso (inclusi quelli "nascosti" dentro software gestionali, CRM, HR e strumenti di marketing). — INVENTARIO
- ☐ ☐ ☐ Abbiamo verificato la presenza di "shadow AI": strumenti (ChatGPT, Copilot, Gemini…) usati dai dipendenti senza autorizzazione o policy aziendale. — SHADOW AI
- ☐ ☐ ☐ Per ogni sistema abbiamo identificato il nostro ruolo ai sensi dell'AI Act: fornitore, deployer (utilizzatore), importatore o distributore: gli obblighi cambiano radicalmente. — ART. 3
- ☐ ☐ ☐ Sappiamo se una personalizzazione o rebranding di un sistema di terzi ci trasforma da semplici utilizzatori a "fornitori" (con tutti gli obblighi che ne derivano). — ART. 25
- ☐ ☐ ☐ Ogni sistema è stato classificato per livello di rischio (vietato / alto rischio / rischio di trasparenza / rischio minimo) con motivazione scritta. — ART. 6
- ☐ ☐ ☐ Se riteniamo che un sistema usato in ambiti dell'Allegato III non sia ad alto rischio, l'autovalutazione è documentata ed è pronta per la futura registrazione nella banca dati UE. — ART. 6(3)
- ☐ ☐ ☐ L'inventario ha un owner e una procedura di aggiornamento: ogni nuovo acquisto o attivazione di AI passa da una valutazione preventiva. — PROCESSO

⚠ **Punto critico.** Nella nostra esperienza, il primo censimento fa emergere in media il doppio dei sistemi AI rispetto a quelli che l'azienda pensava di usare. La classificazione del rischio è l'errore più costoso da sbagliare: da lì discendono tutti gli altri obblighi.

2 Pratiche vietate

IN VIGORE

Art. 5 · in vigore dal 2 feb 2025 · sanzioni fino a 35 mln € o 7% del fatturato

- ☐ ☐ ☐ Abbiamo verificato che nessun sistema utilizzi tecniche manipolative o subliminali che distorcono in modo dannoso il comportamento di clienti o utenti. — ART. 5(1)A
- ☐ ☐ ☐ Nessun sistema sfrutta le vulnerabilità di persone dovute a età, disabilità o condizione socio-economica. — ART. 5(1)B
- ☐ ☐ ☐ Non usiamo forme di social scoring che producano trattamenti pregiudizievoli ingiustificati verso persone o gruppi. — ART. 5(1)C
- ☐ ☐ ☐ Non usiamo il riconoscimento delle emozioni sul luogo di lavoro o in ambito educativo (attenzione a software HR e strumenti di monitoraggio importati da mercati extra-UE). — ART. 5(1)F
- ☐ ☐ ☐ Non usiamo categorizzazione biometrica per dedurre dati sensibili (origine etnica, opinioni politiche, orientamento sessuale…) né scraping indiscriminato di immagini facciali. — ART. 5(1)E,G
- ☐ ☐ ☐ Il divieto di generare deepfake intimi non consensuali e materiale pedopornografico tramite AI è già introdotto dal Digital Omnibus, con applicazione piena dal 2 dic 2026: nessuno dei nostri strumenti lo consente. — OMNIBUS

⚠ **Punto critico.** Il divieto colpisce anche chi usa il sistema, non solo chi lo produce. Alcune funzioni vietate (es. emotion recognition) sono presenti "di serie" in software commerciali del tutto legittimi in altri mercati.

Gli obblighi scattati il 2 agosto: trasparenza e formazione

3 Trasparenza verso utenti e pubblico

IN VIGORE

Art. 50 · applicabile dal 2 ago 2026 · [Fornitore] obbligo di chi produce il sistema, [Deployer] obbligo di chi lo usa

☐ ☐ ☐	Ogni chatbot o assistente virtuale dichiara che si sta interagendo con un'AI, salvo sia già evidente per una persona ragionevolmente informata (un generico pulsante "Chat" non basta).	DEPLOYER · ART. 50(1)
☐ ☐ ☐	I contenuti sintetici (audio, immagini, video, testo) sono marcati in un formato leggibile dalla macchina (metadati, watermark): una semplice dicitura visibile "generato con AI" da sola non soddisfa l'obbligo.	FORNITORE · ART. 50(2)
☐ ☐ ☐	I deepfake (persone, luoghi o eventi reali mostrati in modo falsato) sono etichettati come generati o manipolati artificialmente.	DEPLOYER · ART. 50(4)
☐ ☐ ☐	I testi pubblicati per informare il pubblico, se generati con AI, lo dichiarano, salvo revisione umana e responsabilità editoriale, che vanno però documentate.	DEPLOYER · ART. 50(4)
☐ ☐ ☐	Se usiamo (dove lecito) sistemi di riconoscimento delle emozioni o categorizzazione biometrica, le persone esposte al sistema ne sono informate.	DEPLOYER · ART. 50(3)
☐ ☐ ☐	Le informative sono fornite al più tardi alla prima interazione o esposizione, in modo chiaro, distinguibile e accessibile, non nascoste in fondo a termini e condizioni.	DEPLOYER · ART. 50(5)
☐ ☐ ☐	Abbiamo verificato come i fornitori dei nostri strumenti implementano la marcatura, e cosa resta a nostro carico come deployer.	DEPLOYER · FORNITORI
☐ ☐ ☐	Abbiamo mappato il regime transitorio: i sistemi generativi già sul mercato prima del 2 ago 2026 hanno tempo fino al 2 dic 2026 per la marcatura; i nuovi devono essere conformi da subito.	FORNITORE · TRANSITORIO

⚠ **Punto critico.** È l'area dove la non conformità è visibile a chiunque con una visita al tuo sito. Attenzione però a non marcare tutto: la semplice assistenza all'editing è esclusa dall'obbligo, ma il confine tra assistenza e generazione va valutato caso per caso.

4 Alfabetizzazione AI del personale

IN VIGORE

Art. 4 · in vigore dal 2 feb 2025 · il Digital Omnibus ne ha attenuato la formulazione (da "garantire" a misure per promuovere), ma la responsabilità resta in capo all'organizzazione

☐ ☐ ☐	Il personale che usa o gestisce sistemi di AI ha ricevuto formazione adeguata a ruolo, contesto d'uso e persone impattate.	ART. 4
☐ ☐ ☐	La formazione è differenziata: chi sviluppa, chi decide, chi usa quotidianamente e chi supervisiona hanno bisogni diversi.	RUOLI
☐ ☐ ☐	Esiste un registro della formazione erogata (date, contenuti, partecipanti): in caso di contestazione, poter dimostrare il percorso vale quanto averlo svolto.	EVIDENZE
☐ ☐ ☐	Esiste una policy interna sull'uso dell'AI comunicata a tutto il personale: strumenti ammessi, dati che non si possono inserire, controlli richiesti sugli output.	POLICY
☐ ☐ ☐	La formazione viene aggiornata quando cambiano gli strumenti, i casi d'uso o la normativa (come è appena accaduto con il Digital Omnibus).	CICLO

Governance interna e intreccio con il GDPR

5 Governance e responsabilità

DA FARE ORA

Impostazione organizzativa · art. 2086 c.c. · assetti adeguati e responsabilità degli amministratori

- ☐ ☐ ☐ È stato individuato un responsabile interno per la conformità AI (o un comitato), con mandato, budget e riporto alla direzione. — RUOLO
- ☐ ☐ ☐ Il vertice aziendale (CdA, amministratore) è stato informato formalmente dei rischi AI Act: la vigilanza rientra negli assetti adeguati richiesti dal codice civile. — 2086 C.C.
- ☐ ☐ ☐ Esiste una procedura di approvazione per l'adozione di nuovi sistemi o casi d'uso AI, con valutazione preventiva di rischio e conformità. — PROCESSO
- ☐ ☐ ☐ Esiste una procedura per incidenti e malfunzionamenti legati all'AI: chi interviene, chi valuta, come si documenta, quando si sospende il sistema. — INCIDENTI
- ☐ ☐ ☐ Gli output rilevanti dell'AI sono sottoposti a controllo umano prima di produrre effetti su clienti, dipendenti o terzi (decisioni, comunicazioni, prezzi, valutazioni). — OVERSIGHT
- ☐ ☐ ☐ La conformità AI è coordinata con le altre funzioni: DPO/privacy, legale, IT security, HR, evitando silos e documentazione contraddittoria. — COORD.
- ☐ ☐ ☐ Sappiamo chi ci controlla in Italia: ACN è l'autorità di vigilanza del mercato (ispezioni e sanzioni), AgID l'autorità di notifica, e sappiamo chi in azienda risponderebbe a una loro richiesta. — L. 132/2025

6 Dati personali: dove AI Act e GDPR si incontrano

IN VIGORE

GDPR · Art. 27 AI Act (FRIA) · le autorità privacy sono già pienamente operative sull'AI

- ☐ ☐ ☐ Per ogni trattamento di dati personali tramite AI esiste una base giuridica identificata e un'informativa aggiornata che menziona l'uso dell'AI. — GDPR
- ☐ ☐ ☐ Dove l'AI comporta rischi elevati per le persone è stata svolta (o aggiornata) la DPIA, che oggi deve considerare anche i rischi specifici dell'AI. — ART. 35
- ☐ ☐ ☐ Se siamo banca, assicurazione o soggetto pubblico, sappiamo che ci attende la FRIA (valutazione d'impatto sui diritti fondamentali) e conosciamo il coordinamento FRIA-DPIA introdotto dall'Omnibus. — DIC 2027 — ART. 27
- ☐ ☐ ☐ Le decisioni automatizzate con effetti significativi sulle persone (credito, selezione, profilazione) rispettano l'art. 22 GDPR: intervento umano, contestazione, spiegazione. — ART. 22
- ☐ ☐ ☐ Sappiamo quali dati aziendali finiscono nei sistemi AI dei fornitori (prompt, documenti caricati, dati clienti) e se vengono usati per addestrare i loro modelli. — FLUSSI
- ☐ ☐ ☐ L'uso di AI verso i dipendenti (monitoraggio, valutazione, selezione) è stato verificato anche rispetto all'art. 88 GDPR, allo Statuto dei lavoratori e agli obblighi informativi. — ART. 88

⚠ **Punto critico.** Il rinvio degli obblighi "alto rischio" al 2027 non sospende il GDPR: un sistema di selezione del personale o di scoring creditizio produce già oggi piena responsabilità sotto la normativa privacy e giuslavoristica.

Fornitori, contratti e la roadmap verso il 2027–2028

7 Catena di fornitura e contratti

DA FARE ORA

Artt. 25, 28 e ss. · la conformità dei tuoi fornitori non ti solleva dalle tue responsabilità

- ☐ Abbiamo mappato i fornitori di AI (inclusi i modelli GPAI integrati nei loro prodotti) e raccolto la loro documentazione di conformità all'AI Act. — SUPPLY
- ☐ I contratti con i fornitori AI includono clausole su conformità AI Act, obblighi informativi, cooperazione con le autorità e allocazione delle responsabilità. — CONTRATTI
- ☐ Sappiamo cosa succede ai nostri obblighi se modifichiamo, personalizziamo o rimarchiamo il sistema di un fornitore (rischio di riqualificazione come "fornitore"). — ART. 25
- ☐ Esiste una strategia di uscita: se un fornitore risulta non conforme o dismette il prodotto, sappiamo come sostituirlo senza bloccare i processi. — EXIT
- ☐ Se partecipiamo a bandi e incentivi (es. Transizione 5.0, credito R&S), abbiamo verificato che le spese in AI siano riferite a sistemi conformi: la non conformità può far decadere il beneficio. — INCENTIVI

8 Prepararsi all'alto rischio (senza aspettare il 2027)

2027–2028

Capo III, Sez. 1–3 · Art. 26 (obblighi deployer) · applicabile dal 2 dic 2027 (Allegato III) e dal 2 ago 2028 (Allegato I)

- ☐ Sappiamo quali dei nostri sistemi ricadranno nel regime alto rischio: HR e selezione, credito e scoring, istruzione, biometria, infrastrutture critiche, dispositivi regolamentati. — ALL. III/I
- ☐ Abbiamo svolto una gap analysis rispetto ai futuri requisiti (art. 26 per i deployer): uso secondo le istruzioni del fornitore, sorveglianza umana, monitoraggio, conservazione dei log, qualità dei dati. — ART. 26
- ☐ I lavoratori interessati dall'uso di sistemi ad alto rischio saranno informati secondo le procedure previste (e le relazioni sindacali sono state considerate). — LAVORO
- ☐ Abbiamo pianificato tempi e budget: i requisiti alto rischio richiedono in media 12–18 mesi di preparazione tra processi, documentazione e adeguamenti tecnici. — PIANO
- ☐ Nei nuovi acquisti di sistemi destinati ad ambiti sensibili chiediamo già oggi ai fornitori garanzie di conformità ai futuri requisiti (per non comprare un problema). — PROCURE
- ☐ Seguiamo l'evoluzione di norme armonizzate, linee guida della Commissione e prassi dell'autorità italiana, che definiranno il "come" operativo dei requisiti. — MONITOR
- ☐ Il rinvio al 2027–2028 è trattato come tempo da investire, non come rinvio del problema: c'è un piano trimestrale con responsabili e milestone. — ROADMAP

⚠ **Punto critico.** Chi ha rimandato tutto "perché tanto se ne parla nel 2027" arriverà alla scadenza con gli stessi 12–18 mesi di lavoro, ma senza più margine. Le aziende che si muovono ora trasformano la conformità in argomento commerciale verso clienti e capofila.

Non sai quali dei tuoi sistemi finiranno in "alto rischio"? È la domanda giusta da cui partire, e la risposta richiede un'analisi caso per caso, non una regola generale.

Parliamone → yellowtech.it/contattaci

AUTOVALUTAZIONE

Conta i tuoi ✓ e scopri dove sei davvero

La checklist contiene 51 punti di controllo. Conta quanti ne hai segnati con ✓ (fatto e documentato) e leggi la fascia corrispondente. Ricorda: ogni "?" conta come zero.

0–20

ESPOSIZIONE ALTA

L'azienda usa AI senza presidi verificabili, in una fase in cui vigilanza e sanzioni sono già operative. Priorità assoluta: censimento, trasparenza Art. 50 e verifica delle pratiche vietate. Da affrontare nelle prossime settimane, non nei prossimi mesi.

21–37

CONFORMITÀ PARZIALE

Ci sono basi, ma con lacune che un controllo farebbe emergere subito: tipicamente su evidenze documentali, contratti con i fornitori e formazione. Serve chiudere i gap in modo ordinato, partendo da ciò che è già in vigore.

38–51

BUONA BASE

Il lavoro impostato è solido. I punti aperti sono quasi sempre i più tecnici: classificazione dei casi dubbi, preparazione all'alto rischio, coordinamento FRIA-DPIA. Una verifica indipendente serve a validare (e certificare ai clienti) quanto fatto.

→ Cosa questa checklist non può fare per te

Una checklist ti dice cosa verificare, non come risolvere il tuo caso specifico. La classificazione di rischio di un sistema, la riscrittura di un contratto di fornitura, la marcatura tecnica dei contenuti o l'autovalutazione da registrare in banca dati UE dipendono dal tuo settore, dai tuoi strumenti e dai tuoi dati. È esattamente il lavoro che facciamo ogni giorno con le aziende italiane.

CHI SI AFFIDA A NOI

Bocconi · Politecnico di Milano · HYPE · WEROAD · LEXROOM

Prenota il tuo AI Act Compliance Check: 30 minuti, gratuito

Porta la checklist compilata: la esaminiamo insieme e ti restituiamo tre priorità operative concrete per la tua azienda, una stima realistica di tempi ed effort, e una risposta chiara ai tuoi casi dubbi. Nessun impegno, nessun preventivo non richiesto.

Oppure scrivici: info@yellowtech.it · yellowtech.it

Yellow Tech

Prenota la call →
yellowtech.it/contattaci