PAN · SENIOR ADVISOR AI

EU AI Act Readiness Checklist

Sai davvero se la tua azienda è in regola con la deadline del 2 agosto 2026? Trenta domande in quindici minuti per scoprirlo.

Angelo Pallanca · pallanca.info

Aprile 2026

Sai davvero se la tua azienda è in regola? Trenta domande in quindici minuti per scoprirlo.

Perché ti serve. Perché ora.

Il **2 agosto 2026** entrano in vigore gli obblighi del Regolamento UE 2024/1689 (“EU AI Act”) sui sistemi AI classificati ad **alto rischio** (Annex III). La sanzione massima per non conformità è **€35 milioni o il 7% del fatturato annuo globale**, qualunque sia il maggiore.

Il problema non è la regolamentazione in sé. Il problema è che oltre la metà delle aziende europee non ha un inventario sistematico dei propri sistemi AI in produzione. Non per negligenza. Perché AI si è diffuso negli ultimi due anni in modo capillare, dentro applicazioni HR, dentro CRM, dentro tool di marketing, dentro processi di credit scoring, e nessuno ha mai fatto la mappatura.

Anche prima della sanzione, una richiesta di audit dal regolatore o dal Garante può bloccare un sistema in produzione. Il regolatore europeo userà i primi due anni come anni “di esempio”: i casi che andranno in stampa serviranno a definire la giurisprudenza. Non vuoi essere uno dei casi-esempio.

> **Chi dovrebbe leggere questo documento.** General Counsel, Chief Information Officer, Chief Risk Officer, Compliance Officer di aziende EU con sistemi AI in produzione in settori regolamentati: banking, insurance, healthcare, HR tech, edtech, scoring, controllo accessi, education.

Come usare il checklist

- **Trenta domande** in **sei sezioni** tematiche.
- Per ogni domanda: rispondi **Sì** / **No** / **Non lo so**.
- **Scoring**: ogni “No” o “Non lo so” vale 1 punto sul tuo gap score.
- Alla fine, sommi i punti delle sei sezioni e leggi l’interpretazione nella pagina finale.
- **Tempo stimato**: 12-18 minuti se rispondi onestamente. Le risposte richiedono che tu sappia cosa succede nei tuoi sistemi, non che tu sia esperto di legge.
- Conviene compilarlo insieme al tuo CIO, al DPO, e a un rappresentante legal.

Sezione 1 — Identificazione & inventario dei sistemi AI

Articolo di riferimento: Art. 3, Art. 25 (provider chain)

1. Hai un **inventario formale** dei sistemi AI usati o sviluppati dalla tua azienda, aggiornato negli ultimi sei mesi?

2. Hai mappato i sistemi AI **dentro fornitori terzi** (HR tech, CRM, marketing automation, identity provider, fraud detection)?

3. Sai distinguere i sistemi AI **ad alto rischio** dagli altri secondo i criteri Annex III (8 aree: biometria, infrastrutture critiche, education, lavoro, servizi essenziali, law enforcement, migrazione, giustizia & democrazia)?

4. Hai identificato il tuo ruolo per ogni sistema secondo l'AI Act: **provider**, **deployer**, **importer**, **distributor**?

5. Hai un **processo formale** per aggiornare l'inventario quando viene introdotto, modificato sostanzialmente o disattivato un sistema AI?

Sezione 2 — Classificazione del rischio

Articolo di riferimento: Art. 5 (proibite), Art. 6 (alto rischio), Annex III

6. Hai **classificato ogni sistema AI** nelle quattro categorie del Regolamento: **proibito**, **alto rischio**, **rischio limitato**, **rischio minimo**?

7. Per ogni sistema ad alto rischio, hai documentato il **caso d'uso specifico** secondo il punto Annex III pertinente?

8. Hai verificato che nessuno dei tuoi sistemi rientri nelle **pratiche proibite** dell'Articolo 5 (manipolazione subliminale, social scoring generale, riconoscimento emozioni in luoghi di lavoro, ecc.)?

9. Hai un **processo di review periodica** della classificazione (almeno annuale o al cambio del caso d'uso)?

10. Sai distinguere un **General-Purpose AI Model (GPAI)** da un **High-risk AI System** secondo l'Articolo 51 e seguenti, e hai capito quale set di obblighi si applica?

Sezione 3 — Conformity & documentazione tecnica

Articolo di riferimento: Art. 8-15, Annex IV

11. Per ogni sistema ad alto rischio, hai un **risk management system** documentato (Art. 9): identificazione, stima, valutazione, mitigazione dei rischi?

12. Hai una **data governance policy** specifica per i dataset di training, validation e test usati nei sistemi ad alto rischio (Art. 10)?

13. Hai **technical documentation completa** secondo Annex IV per ogni sistema ad alto rischio (architettura, scopo, hardware, training data, performance metrics, validation, ecc.)?

14. Hai **automated record-keeping (logging)** attivo sui sistemi ad alto rischio, con retention policy che permetta tracciabilità dei principali eventi (Art. 12)?

15. Hai un **conformity assessment procedure** definito (interno via Annex VI o tramite notified body via Annex VII) per i sistemi ad alto rischio?

Sezione 4 — Trasparenza & informazione

Articolo di riferimento: Art. 13, Art. 50, Art. 52

16. Per i sistemi che **interagiscono con persone fisiche** (chatbot, assistenti, agent), hai informato chiaramente gli utenti che stanno interagendo con AI (Art. 50)?

17. Per i contenuti **AI-generated o manipolati** (testo, immagini, audio, video, deepfake), hai un sistema di **marking, watermarking o disclosure** (Art. 50.2)?

18. Per ogni sistema ad alto rischio, hai **instructions for use** chiare per il deployer, scritte secondo i requisiti Articolo 13?

19. Hai pubblicato (dove richiesto per la tua categoria di provider) le informazioni necessarie sul **registro EU dei sistemi AI ad alto rischio** (Art. 71)?

20. Hai un **processo per gestire le richieste di trasparenza** dai data subjects o dai loro rappresentanti, in coordinamento con la tua compliance GDPR?

Sezione 5 — Human oversight, accuracy & robustness

Articolo di riferimento: Art. 14, Art. 15, Art. 73

21. Per ogni sistema ad alto rischio, hai definito **interventi umani specifici** (kill switch, override, possibilità di non-utilizzo) accessibili a chi ha autorità reale?

22. Le persone designate per fare **human oversight** hanno training adeguato sulle limitazioni del sistema e autorità formale per intervenire?

23. Hai **accuracy, robustness e cybersecurity** testati e documentati secondo metriche pertinenti per i sistemi ad alto rischio (Art. 15)?

24. Hai un **post-market monitoring system** attivo per rilevare malfunzionamenti, drift di performance, casi anomali (Art. 72)?

25. Hai un **incident reporting system** per serious incidents (Art. 73): processi, ruoli, tempi (15 giorni standard, 2 giorni per casi critici), connessione con autorità nazionali competenti?

Sezione 6 — Governance interna & compliance organizzativa

Articolo di riferimento: Art. 4, Art. 26, Art. 27 (FRIA)

26. Hai un **AI compliance officer** designato, oppure un comitato AI Act formalmente costituito con responsabilità chiare?

27. Tutti i dipendenti che progettano o usano sistemi AI hanno **AI literacy training** adeguato al loro ruolo (Art. 4, in vigore dal 2 febbraio 2025)?

28. Hai **rivisto i contratti con i fornitori AI** per includere clausole AI Act (responsabilità, accesso a documentazione, supporto in caso di audit, indemnification)?

29. Hai un **budget allocato** e una **roadmap di compliance** con milestone fino al 2 agosto 2026, approvata dal CdA o dal management equivalente?

30. Per i sistemi ad alto rischio in settori regolamentati, hai completato (o pianificato) la **Fundamental Rights Impact Assessment (FRIA)** richiesta dall'Articolo 27?

Interpreta il tuo gap score

Somma tutti i “No” + “Non lo so” delle sei sezioni. Cerca il tuo punteggio nella tabella.

SCORE	STATUS	INTERPRETAZIONE
0–3	Mature	Sei avanti rispetto alla maggior parte delle aziende EU. Probabilmente ti basta un audit puntuale per chiudere gli ultimi gap formali e produrre la documentazione finale. Tempo stimato per essere pronti il 2 agosto: 3–4 settimane.
4–10	Partially ready	Sei in zona “compliance possibile entro la deadline con sforzo focalizzato”. Probabilmente hai gap concentrati su 1-2 sezioni specifiche (spesso Sezione 3 e Sezione 5). Audit + remediation, 8-10 settimane.
11–20	Significant gap	Rischio reale di non arrivare in tempo. Devi cominciare la remediation **adesso**, non a luglio. Inventario sistemi AI in 2 settimane, gap analysis in altre 3, remediation in 8-10 settimane. Tempo è quasi finito.
21–30	Critical	La compliance per il 2 agosto 2026 è dubbia con risorse interne. Servono due decisioni: (a) investimento immediato in advisor + remediation (ordine di grandezza €50-150k tra fee, tools, ore interne), oppure (b) accettazione formale del rischio sanzionatorio per i sistemi più impattanti, documentata dal CdA. Non c’è una terza via.

Cosa fare adesso, in base al tuo livello

Se sei mature (0-3)

Focus su tre cose: **monitoring continuo** (un report trimestrale al CdA sullo stato AI), **completamento documentazione** (Annex IV per ogni sistema), e **post-market vigilance** attiva. Probabilmente non ti serve consulenza esterna: ti serve disciplina interna.

Se sei partially ready (4-10)

Identifica le 2-3 sezioni dove hai più “No”. Tipicamente sono Sezione 3 (documentazione tecnica) e Sezione 5 (human oversight & robustness). Pianifica un audit di 3 settimane ad aprile-maggio 2026 per chiudere i gap formali, poi 8 settimane di remediation interna. Senza esterni, è fattibile se hai un PMO competente.

Se sei significant gap (11-20)

Ingaggia un advisor entro maggio 2026. La sequenza: inventario completo dei sistemi AI (2 settimane), gap analysis dettagliata per sistema (3 settimane), action plan con prioritizzazione e budget (1 settimana), poi remediation (8-10 settimane). Senza advisor esterno è realisticamente troppo tardi.

Se sei critical (21-30)

Devi prendere una decisione di livello board entro il prossimo CdA. Tre scenari da valutare con CFO e Legal: investimento immediato per provare a chiudere entro agosto, scope-down (disabilitare i sistemi più rischiosi, accettare perdita di funzionalità, ritornare in regola), oppure accettazione documentata del rischio (richiede comunque advisor per minimizzare l'esposizione e preparare la difesa in caso di richiesta del regolatore).

Glossario AI Act (12 termini chiave)

Provider — soggetto che sviluppa o fa sviluppare un sistema AI, lo immette sul mercato o lo mette in servizio sotto il proprio nome o marchio. (Art. 3)

Deployer — soggetto che usa un sistema AI sotto la propria autorità nell'ambito di un'attività professionale (escluso uso personale non professionale). (Art. 3)

Annex III — lista degli otto domini in cui i sistemi AI sono classificati ad alto rischio: biometria, infrastrutture critiche, education, lavoro, servizi essenziali, law enforcement, migrazione, giustizia & democrazia.

High-risk AI — sistemi AI che rientrano nei criteri di Articolo 6 o sono listati in Annex III. Soggetti agli obblighi più rigorosi del Regolamento.

Conformity assessment — procedura per dimostrare che un sistema ad alto rischio rispetta i requisiti dell'AI Act. Può essere interna (Annex VI) o tramite notified body (Annex VII), a seconda della categoria.

Notified body — ente terzo accreditato per condurre conformity assessment esterni dei sistemi AI ad alto rischio.

Post-market monitoring — sistema continuo per raccogliere e analizzare dati sulle performance del sistema AI dopo l'immissione sul mercato, identificare malfunzionamenti, e attivare azioni correttive. (Art. 72)

Substantial modification — cambiamento al sistema AI ad alto rischio che impatta su conformità, performance o uso previsto. Triggera un nuovo conformity assessment. (Art. 43)

General-Purpose AI Model (GPAI) — modello AI addestrato su grandi quantità di dati, capace di svolgere un ampio range di task, integrabile in molti sistemi. Obblighi specifici a partire dal 2 agosto 2025. (Art. 51-55)

Real-time biometric identification — identificazione di persone fisiche tramite dati biometrici in tempo reale o quasi in tempo reale. Generalmente proibita in spazi pubblici, con eccezioni strette per law enforcement. (Art. 5)

Regulatory sandbox — ambiente controllato che permette il testing di sistemi AI innovativi sotto supervisione del regolatore prima dell'immissione sul mercato. Obbligatorio in ogni Stato membro entro il 2026. (Art. 57)

AI literacy — competenze, conoscenze e comprensione che permettono a deployer, provider e persone affected da sistemi AI di farne un uso informato e di comprenderne le opportunità e i rischi. (Art. 4)

Calendario AI Act 2025-2027

DATA	EVENTO
2 agosto 2024	Entrata in vigore del Regolamento
2 febbraio 2025	Obblighi su pratiche proibite (Art. 5) e AI literacy (Art. 4)
2 agosto 2025	Obblighi su General-Purpose AI Models (Art. 51-55), penalties (Art. 99-101), governance authorities
2 agosto 2026	**Obblighi pieni sui sistemi ad alto rischio Annex III** — la deadline che conta per la maggior parte delle aziende
2 agosto 2027	Obblighi sui sistemi ad alto rischio incorporati in prodotti già regolamentati da altri regimi UE (medical devices, automotive, ecc.)

L’autore

Angelo Pallanca (Pan) — Senior advisor AI per leadership team europei. Trent’anni cross-industry. Ha lavorato su progetti AI in produzione per Banche Centrali Africane (compliance AML), Gobierno de Canarias (tourism intelligence), Principato di Monaco (governance AI nel settore pubblico), UNICEF (AI-powered distance learning). Indipendente, no commission da vendor.

Pubblica regolarmente su pallanca.info/blog (firma editoriale “Pan” per My 5 cents).

Hai trovato gap critici?

Se il tuo gap score è sopra 10, vale la pena fare una conversazione di trenta minuti per capire cosa è prioritario nel tuo caso specifico. Non vendo software di compliance, non ho commissioni da vendor di tools AI Act, e se la tua azienda non rientra nello scope dell’AI Act te lo dico esplicitamente in quei trenta minuti.

Richiedi una proposta scritta: pallanca.info/it/proposal **Oppure scrivimi:** angelo@pallanca.info