

Checklist AI Act 2026

CRITERIO DIGITALE / STRUMENTO OPERATIVO

Percorso in 5 minuti + guida di riferimento

Versione 3.1 Aggiornata al 1 settembre 2026

Uno strumento di screening operativo per identificare il percorso rilevante, organizzare le prime verifiche e riconoscere quando servono informazioni del provider o un approfondimento professionale.

NEUTRAL

Limite: La checklist non è un parere legale, non certifica la conformità e non produce una classificazione definitiva del caso.

Tatiana Miroshina Criterio Digitale

Versione 3.1 · cutoff 2026-09-01

Territorio e punto di partenza

Rispondi pensando a un solo use case. La lingua del documento non determina dove si applica la legge: contano l'organizzazione, il ruolo, il mercato, il primo utilizzo e il luogo in cui viene usato l'output.

QS-T01

L'organizzazione che usa il sistema AI è stabilita o si trova nell'UE?

☐ Sì ☐ No ☐ Da verificare

NORMA APPLICABILE

Nota: Se usa il sistema sotto la propria autorità come attività professionale ed è stabilita o si trova nell'UE, il criterio territoriale del deployer è confermato.

Sì → EU core No → domanda 2 Da verificare → raccogli informazioni su organizzazione e controllo del sistema

QS-T02

Se sei fuori dall'UE, esiste un collegamento concreto con il mercato o l'uso nell'UE?

- ☐ un sistema AI o un modello GPAI è immesso sul mercato dell'UE;
- ☐ un sistema AI è messo in servizio nell'UE;
- ☐ l'output prodotto dal sistema AI è utilizzato nell'Unione;
- ☐ un fabbricante immette sul mercato o mette in servizio un sistema AI insieme al proprio prodotto e con il proprio nome o marchio;
- ☐ la fornitura coinvolge un importatore, distributore o rappresentante autorizzato stabilito nell'UE.

☐ Sì ☐ No ☐ Da verificare

Nota: Avere un cliente europeo è un segnale da approfondire, non una risposta giuridica automatica.

L'uso futuro previsto dell'output nell'Unione è solo un segnale da verificare; non conferma da solo un criterio di ingresso dell'Article 2.

Stati del risultato

COLLEGAMENTO TERRITORIALE CONFERMATO: È stato identificato almeno un criterio di ingresso. Continua con ruolo e use case. Non significa che ogni obbligo si applichi.

POSSIBILE COLLEGAMENTO CON L'UE: Alcuni fatti indicano una possibile rilevanza, ma servono contratti, catena di fornitura o dati sul luogo d'uso.

DA VERIFICARE: Mancano informazioni. Non scegliere automaticamente il percorso meno rigoroso.

USO INFORMATIVO: Non emerge un collegamento evidente. Puoi usare la checklist come riferimento, senza concludere che l'AI Act si applichi o non si applichi.

NEUTRAL

Nota legale: Questa pagina determina solo il percorso di screening. Non stabilisce conformità, ruolo definitivo o classificazione high-risk.

Quale percorso seguire?

QS-R01

Usi un servizio AI oppure crei o fornisci una soluzione?

☐ Uso un servizio → Percorso A ☐ Creo o fornisco una soluzione → Percorso C ☐ Fornisco un modello → Percorso C + GPAI ☐ Più di una risposta → combina i percorsi ☐ Da verificare → pagina 06

QS-P01

L'AI decide o raccomanda qualcosa sulle persone?

Nota: Considera lavoro, istruzione, credito, assicurazioni, servizi essenziali, biometria, law enforcement, migrazione, giustizia, salute e prodotti legati alla sicurezza. ☐ Sì → Percorso B ☐ No → continua ☐ Da verificare → Percorso B finché il dubbio resta aperto

QS-A5

Vedi un possibile red flag Article 5?

Nota: Manipolazione o inganno con possibile danno, vulnerabilità, social scoring, alcune pratiche biometriche o di riconoscimento delle emozioni, facial scraping, determinate previsioni del rischio criminale o materiale sessuale sintetico vietato. ☐ Sì → STOP / pagina 07 / legal ☐ No → continua ☐ Da verificare → non procedere come se la risposta fosse negativa

QS-A50

Il sistema interagisce con persone o genera contenuti?

Nota: Interazione diretta, emotion/biometric systems, audio, immagini, video, deepfake o testi destinati al pubblico. ☐ Sì → pagina 11 ☐ No → Article 50 può essere condizionale ☐ Da verificare → chiedi al provider

QS-DATA

Sono coinvolti dati personali, dati sensibili o possibili effetti rilevanti sui diritti? ☐ Sì → pagina 14 ☐ No → documenta perché ☐ Da verificare → data mapping / DPO

QS-A25

Hai cambiato nome, configurazione o finalità del sistema?

Nota: Verifica il tuo marchio, modifiche sostanziali e cambi di intended purpose che possono incidere sulla classificazione high-risk. ☐ Sì → Percorso C / pagina 13 ☐ No → conserva l'evidenza ☐ Da verificare → verifica Article 25

Percorsi A–D

ROUTE-A

PERCORSO A — USO ORDINARIO

Sceglilo se usi un servizio AI già disponibile e non emergono red flags people, high-risk o provider.
Leggi: 06 → 09 → 10 → 11 se pertinente → 14 se ci sono dati → 19
Risultato: scheda dello use case, responsabile, revisione umana, AI literacy e domande al provider.
Quando approfondire: dati sensibili, contenuti di interesse pubblico, decisioni sulle persone o istruzioni insufficienti.

Avanti

ROUTE-B

PERCORSO B — PERSONE / IMPATTO ELEVATO

Sceglilo se l'AI decide, raccomanda, classifica o incide su persone e opportunità.
Leggi: 07 → 08 → 12 → 14 → 19
Risultato: intended purpose, persone interessate, verifica high-risk e sintesi per legal/DPO.
Quando approfondire: Article 5, profiling, HR, credito, biometria, minori, salute o servizi essenziali.

Avanti

ROUTE-C

PERCORSO C — CREO O FORNISCO UNA SOLUZIONE

Sceglilo se sviluppi, vendi, rebrandizzi o fornisci un sistema o un modello.
Leggi: 06 → 08 → 13 → 11 → 12 se pertinente → 19
Risultato: mappa dei ruoli, catena di fornitura, intended purpose e lacune documentali.
Quando approfondire: prima dell'immissione sul mercato se restano dubbi su Article 25, high-risk o GPAI.

Avanti

ROUTE-D

PERCORSO D — FUORI DALL'UE

Sceglilo se l'organizzazione è fuori dall'UE e può esistere un collegamento territoriale.
Leggi: 02 → 06 → quindi A, B o C
Risultato: mappa dei fatti territoriali e stato confermato / possibile / da verificare / informativo.
Quando approfondire: contratti, flusso verso il mercato o uso dell'output non chiari.

Avanti

Esempio di combinazione: Una società extra-UE che vende in Europa un sistema per screening dei candidati può avere i percorsi D + C + B.

NEUTRAL

Disclaimer: Il percorso indica cosa verificare. Non stabilisce che il sistema sia conforme, vietato o high-risk.

Che cosa deve restare dopo lo screening

Checklist

- ☐ ☐ Use case descritto
- ☐ Evidenza: scopo, utenti, persone interessate e responsabile.
- ☐ ☐ Territorio documentato
- ☐ Evidenza: organizzazione, mercato, luogo del primo uso e luogo d'uso dell'output.
- ☐ ☐ Ruolo probabile identificato
- ☐ Evidenza: ipotesi di ruolo e fatti ancora da confermare.
- ☐ ☐ Informazioni del provider raccolte
- ☐ Evidenza: intended purpose, instructions, limiti e documentazione disponibile.
- ☐ ☐ Article 5 verificato
- ☐ Evidenza: nessun segnale / possibile segnale / necessità di approfondimento.
- ☐ ☐ Article 6 verificato
- ☐ Evidenza: Annex I/III, Article 6(3), profiling e ruolo.
- ☐ ☐ AI literacy organizzata
- ☐ Evidenza: persone, misure, responsabile e data.
- ☐ ☐ Article 50 verificato
- ☐ Evidenza: interazione/output, ruolo e decisione su informativa o marcatura.
- ☐ ☐ Dati e diritti verificati
- ☐ Evidenza: data inventory e DPIA/FRIA status.
- ☐ ☐ Azioni aperte assegnate
- ☐ Evidenza: domanda, responsabile, interlocutore e scadenza.

Metodo compatto

- ☐ Analizza un use case alla volta.
- ☐ Se una risposta è incerta, usa DA VERIFICARE.
- ☐ Se cambia ruolo, finalità o sistema, ripeti lo screening.
- ☐ Separa obbligo legale, guidance e pratica operativa.
- ☐ Lo screening non è una qualificazione legale.

Legenda

- ☐ LEGGE APPLICABILE: Obbligo applicabile al cutoff.
- ☐ OBBLIGO FUTURO: Norma adottata, con applicazione successiva.
- ☐ GUIDA UFFICIALE: Chiarimento non vincolante della Commissione.
- ☐ PRATICA OPERATIVA: Misura organizzativa utile, non obbligo universale.
- ☐ DA VERIFICARE: Informazioni insufficienti o qualificazione specialistica necessaria.

Quando si applicano le regole

NEUTRAL

Non iniziare da questa pagina. Prima scegli il percorso nelle pagine 02-03; poi usa la timeline per distinguere ciò che vale oggi da ciò che richiede preparazione.

NOW

01.08.2024: Entrata in vigore dell'AI Act.

02.02.2025: Definizioni, Article 4 e otto divieti originari.

02.08.2025: GPAI, governance e quadro sanzionatorio nazionale.

27.07.2026: Regulation (EU) 2026/1744 entra in vigore.

02.08.2026: Article 50, principali norme residue ed enforcement.

PROSSIMAMENTE

02.12.2026: Due nuovi divieti Article 5 e transizione limitata per determinati sistemi ai fini di Article 50(2).

02.08.2027: Termine transitorio per i modelli GPAI immessi sul mercato prima del 2 agosto 2025; sandbox nazionale.

LATER

02.12.2027: Chapter III, Sections 1-3 per Article 6(2) / Annex III.

02.08.2028: Chapter III, Sections 1-3 per Article 6(1) / Annex I.

Una data da sola non basta: verifica sempre articolo, ruolo, categoria, condizioni ed eventuali transizioni.

S1 — Article 113; S2; S3

Quale ruolo hai in questo use case?

Una stessa organizzazione può avere più ruoli in use case diversi. Il ruolo descrive ciò che fai con una specifica soluzione, non l'identità generale dell'azienda.

DEPLOYER: Usi un sistema AI sotto la responsabilità della tua organizzazione. Il semplice uso personale e non professionale è escluso da questa definizione.

PROVIDER DI UN SISTEMA AI: Sviluppi o fai sviluppare un sistema e lo immetti sul mercato o lo metti in servizio con il tuo nome o marchio.

IMPORTER: Sei stabilito nell'UE e immetti sul mercato un sistema che porta il nome o il marchio di un provider extra-UE.

DISTRIBUTOR: Fai parte della catena di fornitura e rendi disponibile il sistema sul mercato UE senza essere provider o importer.

AUTHORISED REPRESENTATIVE: Sei stabilito nell'UE e hai accettato un mandato scritto da un provider extra-UE. Un cliente o consulente non diventa representative automaticamente.

GPAI PROVIDER: Sviluppi o fai sviluppare un modello AI per finalità generali e lo immetti sul mercato con il tuo nome.

Esempi

- ☐ Usare ChatGPT per una bozza non ti rende provider del modello.
- ☐ Vendere un tuo sistema costruito tramite API può renderti provider del sistema, ma non automaticamente del modello GPAI.
- ☐ La stessa organizzazione può essere deployer in un processo e provider in un altro.

Article 25 — approfondimento

Verifica il trasferimento degli obblighi del provider se: - applichi il tuo nome o marchio a un sistema high-risk; - apporti una modifica sostanziale e il sistema resta high-risk; - cambi l'intended purpose e il sistema diventa high-risk. Non ogni configurazione, integrazione o prompt produce questo effetto.

Un'ipotesi di ruolo, le evidenze che la sostengono e i punti da confermare.

S1 — Articles 3, 25, 53 e 54

C'è un red flag da fermare e verificare?

NEUTRAL

Se emerge una possibile corrispondenza: FERMA / VERIFICA / APPROFONDISCI. Non continuare la messa in uso come se il risultato fosse negativo.

Applicabile ora

NORMA APPLICABILE

1. Manipolazione o inganno con danno significativo o ragionevolmente probabile.
2. Sfruttamento di età, disabilità o condizione socioeconomica con danno.
3. Social scoring con trattamento sfavorevole non pertinente o sproporzionato.
4. Predizione del rischio criminale individuale basata soltanto su profiling o tratti.
5. Raccolta non mirata di immagini facciali da internet o CCTV.
6. Inferenza delle emozioni in lavoro o istruzione, salvo specifiche eccezioni.
7. Biometric categorisation relativa a determinati attributi sensibili o protetti.
8. Identificazione biometrica remota in tempo reale in spazi pubblici per attività di contrasto, salvo condizioni ed eccezioni strette.

Futuro dal 2 dicembre 2026

NORMA FUTURA

Determinati sistemi che generano o manipolano materiale intimo o sessualmente esplicito riferito a una persona identificabile senza il consenso richiesto.

Determinati sistemi che generano o manipolano materiale di abuso sessuale su minori senza diritto.

Che cosa fare

- ☐ Sospendi l'estensione del use case.
- ☐ Conserva intended purpose, input, output, utenti e persone interessate.
- ☐ Verifica il testo completo, condizioni, soglie ed eccezioni.
- ☐ Coinvolgi legal e, se pertinente, DPO o specialisti settoriali.

NEUTRAL

Limite: Questa pagina riconosce segnali. Non produce una qualificazione definitiva di pratica vietata.

S1 — Article 5; S2; S3; S4

Questo use case richiede il test high-risk?

NEUTRAL

Se sei nel Percorso A e nessuno dei segnali sotto è presente, registra il risultato e puoi rimandare il dettaglio. Se una risposta è “sì” o “da verificare”, passa al Percorso B o C.

A / Annex I

NORMA FUTURA

Il sistema è un componente di sicurezza o un prodotto disciplinato dall'Annex I e soggetto a valutazione della conformità da parte di terzi?

B / Annex III

NORMA FUTURA

L'intended purpose riguarda biometria, infrastrutture critiche, istruzione, lavoro, servizi essenziali, attività di contrasto, migrazione o giustizia/processi democratici?

C / Article 6(3)

Il sistema svolge soltanto un compito procedurale, preparatorio o di pattern detection, senza rischio significativo e senza influenzare materialmente la decisione?

D / Profiling

NORMA FUTURA

Il sistema Annex III effettua profiling di persone fisiche? In questo caso resta high-risk.

E / Ruolo

Sei provider, deployer o un operatore la cui posizione può cambiare ai sensi di Article 25?

Date

NORMA FUTURA

ANNEX III / ARTICLE 6(2): Obblighi dal 2 dicembre 2027.

ANNEX I / ARTICLE 6(1): Obblighi dal 2 agosto 2028.

Nessun segnale identificato / possibile high-risk / da verificare. Nessuno di questi risultati equivale a una classificazione legale definitiva.

Nota: Le linee guida high-risk disponibili alla data di riferimento sono bozze e non vincolanti.

S1 — Articles 6 e 113; S2; S3; S11

Uso ChatGPT, Claude o Gemini: che cosa faccio ora?

☐ Questo percorso è pensato per una piccola organizzazione che usa un servizio AI già disponibile. Alcuni punti derivano dalla legge; altri sono pratiche organizzative prudenti.

LEGAL / VERIFICA APPLICABILE

- ☐ Identifica il tuo ruolo per il singolo use case.
- ☐ Adotta misure contestuali di AI literacy ai sensi di Article 4.
- ☐ Verifica Article 50 quando il sistema interagisce con persone o genera/manipola contenuti.
- ☐ Esegui il primo screening Article 5 e Article 6.
- ☐ Applica GDPR e regole settoriali quando pertinenti.

PRACTICE / ORGANIZZA IL LAVORO

- ☐ Registra strumenti, utenti e finalità.
- ☐ Assegna un responsabile a ogni use case.
- ☐ Conserva instructions, condizioni e limiti del provider.
- ☐ Definisci quali dati non possono essere inseriti.
- ☐ Indica quali output richiedono revisione umana.
- ☐ Definisci un canale di approfondimento e gestione degli incidenti.
- ☐ Registra decisioni e questioni aperte.

Output minimo

CAMPO	EVIDENZA
Tool	Nome, versione/account e provider
Use case	Finalità e processo
Persone	Utenti e persone interessate
Dati	Categorie e restrizioni
Revisione	Chi controlla output e decisioni
Contatto	Chi contattare e quando
Data di revisione	Trigger o scadenza

NEUTRAL

Limite: Un use case “ordinario” può comunque coinvolgere privacy, lavoro, copyright, consumer protection, segreti commerciali o responsabilità contrattuale.

- ☐ S1 — Articles 4, 5, 6, 26 e 50; S5; S9

AI literacy: che cosa richiede davvero la legge?

LEGGE APPLICABILE

NORMA APPLICABILE

Provider e deployer devono adottare misure per sostenere lo sviluppo dell'AI literacy del personale e delle altre persone che operano o usano sistemi AI per loro conto.

Le misure devono considerare conoscenze tecniche, esperienza, formazione, contesto d'uso e persone o gruppi sui quali il sistema viene usato.

NON RICHIEDE AUTOMATICAMENTE

- ☐ un livello numerico garantito per ogni persona;
- ☐ un numero minimo di ore;
- ☐ un certificato;
- ☐ un corso unico per tutti;
- ☐ un AI officer;
- ☐ un DPO o governance board dedicato.

POSSIBILI MISURE OPERATIVE

- ☐ breve formazione sugli strumenti realmente usati;
- ☐ elenco di strumenti e finalità autorizzate;
- ☐ esempi di errori, allucinazioni e rischi;
- ☐ regole per dati personali, riservati e segreti commerciali;
- ☐ revisione umana per output rilevanti;
- ☐ canale di approfondimento e registro essenziale delle iniziative.

Output

Persone coinvolte, misure scelte, motivazione, responsabile, data e prossimo aggiornamento.

NEUTRAL

Nota: La repository di esempi dell'AI Office è una risorsa di apprendimento. Copiarne un esempio non crea automaticamente una presunzione di conformità.

S1 — Article 4; S2; S5

Quale tipo di interazione o output hai?

Article 50 è applicabile dal 2 agosto 2026. Prima identifica soggetto, contenuto e ruolo.

INTERAZIONE DIRETTA — PROVIDER

NORMA APPLICABILE

Il provider progetta il sistema affinché le persone siano informate dell'interazione con AI, salvo quando ciò è evidente per una persona ragionevolmente informata e attenta.

CONTENUTO SINTETICO — PROVIDER

NORMA APPLICABILE

Il provider di sistemi che generano audio, immagini, video o testo sintetici assicura una marcatura machine-readable e rilevabile, con le eccezioni previste.

EMOZIONI / BIOMETRIC CATEGORISATION — DEPLOYER

NORMA APPLICABILE

Il deployer informa le persone esposte al funzionamento del sistema e applica le regole sui dati personali.

DEEPFAKE — DEPLOYER

NORMA APPLICABILE

Il deployer rende noto che il contenuto è generato o manipolato. Per opere artistiche, creative, satiriche o di finzione si applica una modalità adattata.

TESTO DI INTERESSE PUBBLICO — DEPLOYER

NORMA APPLICABILE

Il deployer rende noto l'uso dell'AI quando il testo è pubblicato per informare il pubblico su questioni di interesse pubblico, salvo revisione umana/ controllo editoriale e responsabilità editoriale identificabile.

Transizione

NORMA APPLICABILE

Determinati provider di sistemi già immessi sul mercato prima del 2 agosto 2026 devono adeguarsi ad Article 50(2) entro il 2 dicembre 2026. Non è un rinvio generale di Article 50.

Output

- ☐ tipo di interazione/output;
- ☐ provider o deployer responsabile;
- ☐ exception verificata;
- ☐ evidenza dell'informativa o della marcatura;
- ☐ data della decisione.

NEUTRAL

Limite: Non esiste una formula unica da applicare a ogni contenuto AI.

S1 — Article 50; S2; S3; S9; S10

Se il test high-risk resta aperto o positivo

NEUTRAL

LEGGI SOLO SE IL TUO PERCORSO LO RICHIEDE

Status: Queste disposizioni seguono le date del ramo high-risk: - Annex III: 2 dicembre 2027; - Annex I: 2 agosto 2028. Non sono obblighi universali per ogni uso AI oggi.

PROVIDER

NORMA FUTURA

sistema di gestione del rischio;
governance dei dati;
documentazione tecnica;
registrazione automatica;
informazioni e istruzioni per il deployer;
progettazione della sorveglianza umana;
accuratezza, robustezza e cibersecurity;
sistema di gestione della qualità;
valutazione della conformità;
dichiarazione UE, marcatura CE e registrazione quando applicabili;
monitoraggio successivo all'immissione sul mercato e segnalazione degli incidenti.

DEPLOYER

NORMA FUTURA

uso secondo le istruzioni;
misure tecniche e organizzative adeguate;
persone competenti, formate e autorizzate per la sorveglianza umana;
monitoraggio del funzionamento;
conservazione dei log sotto il proprio controllo;
gestione degli incidenti;
obblighi informativi e di registrazione quando applicabili;
verifica preliminare DPIA e FRIA.

Non confondere Article 14 e Article 26

Article 14 riguarda la progettazione della sorveglianza umana da parte del provider. Article 26 riguarda gli obblighi del deployer. Nessuno dei due crea una procedura scritta universale per ogni uso AI.

Che cosa fare prima della data applicabile

- ☐ documentare intended purpose;
- ☐ chiedere classificazione e istruzioni al provider;
- ☐ verificare il ruolo;
- ☐ identificare lacune nelle evidenze;
- ☐ programmare la preparazione e la verifica delle linee guida finali.

S1 — Articles 8–27 e 113; S2; S11

Creo, integro o fornisco: che cosa sto offrendo?

UTENTE API

Usi un'API o un servizio altrui nel tuo processo. Questo non ti rende automaticamente provider del modello o del sistema originario.

INTEGRATORE / COSTRUTTORE DI SOLUZIONI

NORMA APPLICABILE

Costruisci una soluzione usando componenti o modelli altrui. Puoi diventare provider del tuo sistema se lo offri con il tuo nome, senza diventare automaticamente GPAI provider.

PROVIDER DEL SISTEMA AI

Sviluppi o fai sviluppare un sistema e lo immetti sul mercato o lo metti in servizio con il tuo nome o marchio.

PROVIDER DEL MODELLO GPAI

NORMA APPLICABILE

Sviluppi o fai sviluppare un modello AI per finalità generali e lo immetti sul mercato con il tuo nome.

Article 25 — segnali di trasferimento del ruolo

NORMA FUTURA

Verifica se:

- applichi il tuo nome o marchio a un sistema high-risk;
- apporti una substantial modification;
- cambi l'intended purpose e la soluzione diventa high-risk.

La regola segue le date del relativo ramo high-risk. Puoi però raccogliere ora i fatti e le evidenze.

Se sei GPAI provider

- ☐ documentazione tecnica;
- ☐ informazioni per i provider a valle;
- ☐ politica sul diritto d'autore;
- ☐ sintesi pubblica dei contenuti di addestramento;
- ☐ rappresentante autorizzato quando applicabile.

NORMA APPLICABILE

valutazione del modello e test avversariali;
valutazione e mitigazione del rischio sistemico;
segnalazione degli incidenti;
cibersicurezza.

Date GPAI

NORMA APPLICABILE

2 agosto 2025: obblighi per nuovi modelli;
2 agosto 2026: enforcement;
2 agosto 2027: transizione dei modelli immessi prima del 2 agosto 2025.

Output

Mappa dei ruoli, confine tra prodotto e modello, catena di fornitura, intended purpose, evidenze del provider e domande da sottoporre a specialisti legali/tecnici.

S1 — Articles 3, 25, 51–55; S3; S6; S7; S8; S14

Tre domande diverse

GDPR

Quando verificare: Quando il processo tratta dati personali.

Che cosa controllare: Base giuridica, finalità, minimizzazione, trasparenza, sicurezza, diritti, conservazione e soggetti coinvolti.

Non significa: Usare AI non rende automaticamente lecito o illecito il trattamento.

Specialista: DPO/legal per basi, diritti, trasferimenti e casi sensibili.

DPIA

Quando verificare: Quando il trattamento può comportare un rischio elevato per diritti e libertà.

Che cosa controllare: Necessità, proporzionalità, rischi, misure e rischio residuo.

Non significa: La presenza di AI non rende automaticamente obbligatoria una DPIA.

Specialista: il DPO deve guidare o validare il test quando pertinente.

FRIA

Quando verificare: Per specifici deployer e determinati high-risk systems Article 6(2), tra cui organismi di diritto pubblico, privati che forniscono servizi pubblici e specifici usi in credito e assicurazione.

Che cosa controllare: Processi, persone interessate, effetti sui diritti, sorveglianza umana, governance e rimedi.

NORMA FUTURA

Non significa: Ogni high-risk system o deployer richiede automaticamente una FRIA.

Coordinamento: Le parti già coperte da una DPIA possono essere richiamate o integrate nella FRIA.

Data: Il ramo Annex III è futuro dal 2 dicembre 2027.

Output

NORMA FUTURA

GDPR applicabile? / verifica DPIA / ambito FRIA / responsabile / specialista / questioni aperte.

S1 — Articles 26(9), 27 e 113; S2; S13 — Article 35

PMI non significa esenzione

Le PMI ricevono misure di supporto e alcuni criteri di proporzionalità. Restano soggette agli obblighi che si applicano al loro ruolo e use case.

Supporto

- ☐ accesso prioritario alle sandbox;
- ☐ guidance e formazione adattate;
- ☐ canali con le autorità;
- ☐ sostegno alla standardizzazione;
- ☐ fees ridotte o proporzionate;
- ☐ considerazione di dimensione e capacità economica.

Massimali

VIOLAZIONE	MASSIMALE
Article 5	EUR 35 milioni / 7%
Altri obblighi elencati	EUR 15 milioni / 3%
Informazioni inesatte o fuorvianti	EUR 7,5 milioni / 1%
GPAI	EUR 15 milioni / 3%

SME rule

NORMA APPLICABILE

Per le SME, Article 99(6) applica il minore tra importo assoluto e percentuale alle sanzioni dei paragrafi 3-5.
Article 101 prevede invece una formula separata per GPAI.

Non usare i massimali come previsione

Il massimo non è l'esito normale di ogni errore. Natura, gravità, durata, intenzionalità, cooperazione e circostanze incidono sulla sanzione.

Conclusione operativa

Non calcolare una sanzione con questa pagina. Usala per evitare due errori: credere che una PMI sia esente o trattare ogni mancanza come se producesse automaticamente il massimo.

S1 — Articles 62, 99 e 101; S2; S14

Tre casi dentro l'UE

NEUTRAL

01 / Piccola impresa usa ChatGPT per marketing

Situazione — Impresa italiana usa un servizio disponibile per creare bozze. Una persona approva il contenuto.

Percorso — A

Ruolo probabile — Deployer.

Cosa verificare — Article 4, instructions, dati, revisione umana, Article 50 per il tipo di contenuto.

Cosa non puoi concludere — Che ogni testo richieda un'informativa o che il processo sia già conforme.

Passo successivo — Crea la scheda dello use case e definisci dati ammessi, revisione e criteri di approfondimento.

02 / Screening dei candidati

Situazione — Un employer UE usa AI per classificare CV e raccomandare candidati.

Percorso — B + ordinary deployer.

Ruolo probabile — Deployer; il vendor può essere provider.

Cosa verificare — Article 5, intended purpose, Annex III, Article 6(3), profiling, dati e documentazione del provider.

Cosa non puoi concludere — La classificazione high-risk definitiva senza fatti e documentazione.

Passo successivo — Verifica legal/DPO prima della messa in uso.

03 / Prodotto AI proprio

Situazione — Azienda sviluppa una soluzione e la vende con il proprio marchio sul mercato UE.

Percorso — C; anche D se il provider è extra-UE.

Ruolo probabile — Provider del sistema.

Cosa verificare — Intended purpose, Article 6, Article 25, Article 50, catena di fornitura e documentazione.

Cosa non puoi concludere — Che la soluzione sia automaticamente high-risk o che l'azienda sia GPAI provider.

Passo successivo — Verifica di ruolo e prodotto prima dell'immissione sul mercato.

Contenuti, mercato UE e lingua

NEUTRAL

04 / Contenuto AI destinato al pubblico

Situazione — Organizzazione UE usa AI per generare testi o immagini pubblici.

Percorso — A + Article 50.

Ruolo probabile — Deployer; gli obblighi del provider restano distinti.

Cosa verificare — Marcatura, deepfake, testo di interesse pubblico, revisione umana/editoriale e responsabile identificabile.

Cosa non puoi concludere — Che una formula unica sia obbligatoria per ogni contenuto.

Passo successivo — Documenta la categoria del contenuto, il ruolo e la decisione sull'informativa.

05 / Società extra-UE con clienti europei

Situazione — Società non stabilita nell'UE offre un servizio AI a clienti europei e l'output viene usato nei loro processi.

Percorso — D + possibile C.

Ruolo probabile — Possibile provider; da verificare.

Stato territoriale — Possibile collegamento finché i fatti relativi al mercato e all'output non sono documentati.

Cosa verificare — Prima fornitura, mercato UE, luogo d'uso dell'output, importatore/distributore/ rappresentante autorizzato.

Cosa non puoi concludere — Che la sola presenza di clienti europei renda applicabile ogni obbligo.

Passo successivo — Mappa dei fatti territoriali e verifica specialistica se i contratti non chiariscono il flusso.

06 / Imprenditrice russofona in Italia

Situazione — Professionista russofona vive e lavora in Italia tramite un'attività stabilita nell'UE.

Percorso — Percorso UE determinato dal use case; livello Italia se pertinente.

Ruolo probabile — Deployer, salvo attività aggiuntive.

Stato territoriale — Collegamento territoriale confermato.

Cosa verificare — Gli stessi obblighi applicabili a un'organizzazione equivalente che legge in italiano.

Cosa non puoi concludere — Che la lingua russa implichi un percorso extra-UE.

Passo successivo — Nucleo UE nella lingua più accessibile + livello Italia.

Attuazione nazionale

NEUTRAL

Leggi questa pagina solo se il caso ha un collegamento territoriale rilevante con il paese selezionato.

La lingua italiana non rende automaticamente applicabile il country layer. Verifica establishment, attività, settore e autorità competenti.

Legge applicabile

NORMA APPLICABILE

Legge 23 settembre 2025, n. 132. Pubblicata il 25 settembre 2025 ed entrata in vigore il 10 ottobre 2025. Deve essere interpretata e applicata conformemente al Regulation (EU) 2024/1689.

Autorità

NORMA APPLICABILE

AgID — Autorità di notifica. Svolge funzioni relative a notifica, valutazione, accreditamento e monitoraggio degli organismi di conformity assessment.

ACN — Autorità di vigilanza del mercato e punto di contatto unico, con funzioni ispettive e sanzionatorie secondo la normativa applicabile.

Banca d'Italia / CONSOB / IVASS — Mantengono le competenze di sorveglianza del mercato nei rispettivi ambiti finanziari.

Garante — Restano ferme competenze, compiti e poteri in materia di protezione dei dati personali.

AGCOM e altre autorità — Restano applicabili le competenze previste dall'ordinamento e dal settore.

La legge italiana contiene anche disposizioni settoriali e penali. Non confonderle con i massimali amministrativi degli Articles 99 e 101.

Chi deve fare il passo successivo?

FAI TU

- ☐ descrivi il use case;
- ☐ assegna responsabile e utenti;
- ☐ identifica dati e persone interessate;
- ☐ registra ruolo e stato territoriale;
- ☐ organizza AI literacy;
- ☐ stabilisci la revisione umana;
- ☐ assegna scadenze alle domande aperte.

Scheda dello use case e registro delle azioni.

CHIEDI AL PROVIDER

- ☐ intended purpose e istruzioni;
- ☐ capacità, limiti e rischi noti;
- ☐ conservazione, addestramento e uso dei dati;
- ☐ sicurezza e canale per gli incidenti;
- ☐ registri ed esportazione;
- ☐ marcatura e informativa Article 50;
- ☐ documentazione high-risk/GPAI quando pertinente.

Evidenze tecniche e contrattuali mancanti.

PROCESSI / GOVERNANCE — CRITERIO DIGITALE

- ☐ mappatura dei processi;
- ☐ mappatura degli use case e della catena del valore;
- ☐ controlli operativi;
- ☐ flusso documentale;
- ☐ progettazione della sorveglianza umana;
- ☐ responsabilità e criteri di escalation;
- ☐ registri e architettura di tracciabilità.

NEUTRAL

Confine: Criterio Digitale struttura processi, controlli ed evidenze. Non sostituisce la qualificazione legale.

LEGAL / DPO

- ☐ ambito territoriale complesso;
- ☐ possibile Article 5;
- ☐ classificazione high-risk;
- ☐ Article 25 e obblighi di ruolo;
- ☐ base giuridica e diritti;
- ☐ DPIA e FRIA;
- ☐ contratti, responsabilità e diritto nazionale.

Posizione legale, decisione sulla protezione dei dati o indicazione specialistica.

Regola pratica

Non inviare tutte le domande allo stesso interlocutore. Usa lo stesso fascicolo di fatti ed evidenze, ma assegna ogni questione al soggetto competente.

NEUTRAL

Se l'autoverifica lascia punti aperti, conserva l'elenco: è la sintesi per provider, lavoro su processi/governance e verifica legal/DPO.

Diritto vincolante e principali riferimenti

S1	Regulation (EU) 2024/1689 European Parliament and Council / EUR-Lex Stato: binding Pubblicazione: 2024-07-12 Aggiornamento: 2026-07-27 Entrata in vigore: 2024-08-01 Verificata: 2026-09-01 Fonte ufficiale ↗
S2	Regulation (EU) 2026/1744 European Parliament and Council / EUR-Lex Stato: binding Pubblicazione: 2026-07-24 Entrata in vigore: 2026-07-27 Verificata: 2026-09-01 Fonte ufficiale ↗
S3	Timeline for the Implementation of the EU AI Act European Commission - AI Act Service Desk Stato: non binding Verificata: 2026-09-01 Fonte ufficiale ↗

S4	Guidelines on prohibited artificial intelligence practices European Commission Stato: non binding Pubblicazione: 2025-02-04 Aggiornamento: 2025-07-31 Verificata: 2026-09-01 Fonte ufficiale ↗
S5	AI Literacy — Questions & Answers European Commission / AI Office Stato: non binding Verificata: 2026-09-01 Fonte ufficiale ↗
S6	Guidelines for providers of general-purpose AI models European Commission Stato: non binding Pubblicazione: 2025-07-18 Aggiornamento: 2026-04-20 Verificata: 2026-09-01 Fonte ufficiale ↗

Guidance, strumenti e livello nazionale

NEUTRAL

Una guida, un template o un codice non vincolante non sostituisce il testo del Regulation né l'interpretazione della Corte di giustizia.

S7

General-Purpose AI Code of Practice
European Commission / AI Office
Stato: voluntary
Pubblicazione: 2025-07-10
Aggiornamento: 2026-07-31
Verificata: 2026-09-01
[Fonte ufficiale ↗](#)

S8

Template for the Public Summary of Training Content
European Commission / AI Office
Stato: official tool
Pubblicazione: 2025-07-24
Aggiornamento: 2026-03-26
Verificata: 2026-09-01
[Fonte ufficiale ↗](#)

S9

Guidelines on transparency obligations under Article 50
European Commission
Stato: non binding
Pubblicazione: 2026-07
Aggiornamento: 2026-08-06
Verificata: 2026-09-01
[Fonte ufficiale ↗](#)

S10

Code of Practice on Transparency of AI-generated Content
European Commission / AI Office
Stato: voluntary
Pubblicazione: 2026-06-10
Aggiornamento: 2026-07-31
Verificata: 2026-09-01
[Fonte ufficiale ↗](#)

S11

Guidelines for providers and deployers of high-risk AI systems
European Commission
Stato: draft
Verificata: 2026-09-01
[Fonte ufficiale ↗](#)

S12

Legge 23 settembre 2025, n. 132
Repubblica Italiana / Normattiva
Stato: binding
Pubblicazione: 2025-09-25
Entrata in vigore: 2025-10-10
Verificata: 2026-09-01
[Fonte ufficiale ↗](#)

S13

Regulation (EU) 2016/679 — General Data Protection Regulation (GDPR)
European Parliament and Council / EUR-Lex
Stato: binding
Pubblicazione: 2016-05-04
Entrata in vigore: 2016-05-24
Verificata: 2026-09-01
[Fonte ufficiale ↗](#)

S14

Commission Implementing Regulation (EU) 2026/1755
European Commission / EUR-Lex
Stato: binding
Pubblicazione: 2026-07-21
Verificata: 2026-09-01
[Fonte ufficiale ↗](#)

Versione e prossima revisione

Stato del documento

- ☐ Titolo: Checklist AI Act 2026
- ☐ Versione: 3.1
- ☐ ID edizione: IT / nucleo UE + livello Italia
- ☐ Data di riferimento legale/fattuale: 1 settembre 2026
- ☐ Autrice: Tatiana Miroshina
- ☐ Progetto: Criterio Digitale

Prossima revisione

Entro il 1 dicembre 2026, o prima se cambia una fonte rilevante.

Eventi che richiedono revisione

- ☐ linee guida finali high-risk;
- ☐ atti italiani definitivi di attuazione;
- ☐ atti delegati o di esecuzione rilevanti;
- ☐ aggiornamenti Article 50, GPAI o AI literacy;
- ☐ nuove decisioni della Corte di giustizia;
- ☐ cambiamenti di autorità, procedure o calendario;
- ☐ modifiche che incidono sui percorsi territoriali.

Disclaimer

La checklist è uno strumento operativo di primo orientamento. Non costituisce parere legale, certificazione di conformità o sostituto di una valutazione del caso concreto. Prima di assumere decisioni ad alto impatto, verifica la versione corrente delle fonti e richiedi assistenza professionale quando necessaria.