IL REGOLAMENTO EUROPEO SULL'INTELLIGENZA ARTIFICIALE

AI ACT

Reg. UE 2024/1689

Guida didattica per operatori della Pubblica Amministrazione

Prefazione — Perché studiare l'AI Act oggi

L'intelligenza artificiale non è più una promessa futura: è una realtà operativa che già oggi permea i processi delle pubbliche amministrazioni, delle aziende informatiche e dei fornitori di servizi digitali. Sistemi di riconoscimento documentale, chatbot istituzionali, strumenti di analisi predittiva, motori di raccomandazione per la gestione delle pratiche: tutto questo rientra nell'ambito di applicazione del Regolamento (UE) 2024/1689, entrato in vigore il 1° agosto 2024 con un regime di applicazione progressiva.

Come software house che progetta, sviluppa e integra soluzioni tecnologiche per la pubblica amministrazione, la software house si trova esattamente al crocevia di due ruoli fondamentali previsti dal Regolamento: quello di fornitore (provider) di sistemi AI e quello di deployer (utilizzatore-messo in opera). Comprendere questa duplice posizione è il primo passo per costruire una strategia di compliance solida, credibile e difendibile.

Obiettivo didattico di questa lezione

Al termine di questa sessione formativa, i partecipanti saranno in grado di: identificare il campo di applicazione del Regolamento; classificare un sistema AI in base al livello di

rischio; comprendere gli obblighi applicabili al proprio ruolo; conoscere le principali scadenze del calendario di applicazione; individuare le aree di intersezione con il GDPR.

1. Struttura e architettura del Regolamento

L'AI Act è il primo strumento normativo vincolante al mondo dedicato specificamente all'intelligenza artificiale. Con 180 articoli, 13 allegati tecnici e oltre 1.000 considerando, è un testo di straordinaria complessità sistematica. Tuttavia, la sua architettura è fondata su una logica molto chiara: graduare gli obblighi in funzione del rischio che un sistema AI può generare per le persone e per la società.

1.1 La logica risk-based

Il legislatore europeo ha scelto consapevolmente di non regolamentare la tecnologia in sé, ma gli usi che di essa si fanno e i contesti in cui viene impiegata. Un modello di machine learning utilizzato per ottimizzare il consumo energetico di un edificio è soggetto a obblighi minimi; lo stesso modello, se reimpiegato per valutare le condizioni di accesso a un servizio pubblico, può entrare nella categoria ad alto rischio.

I quattro livelli di rischio

1. Rischio inaccettabile (proibito): sistemi vietati incondizionatamente dall'Articolo 5.
2. Alto rischio: sistemi soggetti a obblighi stringenti prima dell'immissione sul mercato (Allegati II e III).
3. Rischio specifico di trasparenza: sistemi che interagiscono con persone fisiche (chatbot, deepfake generativi) soggetti a obblighi di disclosure.
4. Rischio minimo: la maggioranza dei sistemi AI; nessun obbligo normativo specifico, ma adesione a codici di condotta incoraggiata.

1.2 Definizione di sistema AI: l'Articolo 3

La definizione adottata dal Regolamento (Art. 3, par. 1) è volutamente tecnologicamente neutrale e strettamente allineata alla definizione OCSE:

Definizione normativa

«Sistema di IA»: un sistema automatizzato progettato per funzionare con livelli diversi di autonomia e che può mostrare adattabilità dopo il dispiegamento e che, per obiettivi espliciti o impliciti, deduce, partendo dagli input che riceve, come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali.

Tre elementi qualificanti emergono da questa definizione: (a) l'autonomia operativa, anche parziale; (b) la possibilità di adattamento post-deployment; (c) la capacità di produrre output che influenzano ambienti reali o digitali. La semplice automazione di regole fisse (rule-based)

non integra la definizione, ma attenzione: sistemi ibridi che combinano logica deterministica e componenti apprendimento automatico rientrano nell'ambito.

1.3 Campo di applicazione territoriale

Il Regolamento si applica secondo una logica di effetto (market access principle) analoga al GDPR. È vincolante per:

- i fornitori che immettono sul mercato dell'UE sistemi AI, indipendentemente dalla loro sede legale;
- i deployer stabiliti nell'UE che utilizzano sistemi AI;
- i fornitori e deployer stabiliti fuori dall'UE quando gli output del sistema influenzano persone fisiche nell'UE;
- gli importatori e distributori di sistemi AI;
- i fabbricanti di prodotti che incorporano sistemi AI.

> ⚠ **Rilevanza per i responsabili al trattamento**
>
> In qualità di società italiana che sviluppa soluzioni software per PA italiane ed europee, la software house è soggetta al Regolamento sia come fornitore (quando progetta e commercializza sistemi AI) sia come deployer (quando integra e gestisce tali sistemi nell'operatività quotidiana dei clienti PA). Questa duplice veste comporta il cumulo degli obblighi di entrambe le categorie.

2. I sistemi AI vietati — Articolo 5

L'Articolo 5 del Regolamento individua le pratiche di AI che il legislatore europeo giudica intrinsecamente incompatibili con i valori fondamentali dell'Unione e pertanto vietate in modo assoluto, senza possibilità di deroga. Si tratta di una lista tassativa che si applica dal 2 febbraio 2025, la prima scadenza del calendario di attuazione.

2.1 Le pratiche vietate e il loro razionale

Il Regolamento proibisce le seguenti pratiche, che analizziamo con il commento del loro fondamento valoriale:

a) Manipolazione subliminale e sfruttamento delle vulnerabilità

È vietata la commercializzazione o l'uso di sistemi AI che, ricorrendo a tecniche subliminali o ingannose, manipolano il comportamento di una persona in modo da distorcerne il libero arbitrio, o che sfruttano deliberatamente vulnerabilità legate all'età, a disabilità fisiche o mentali, alla situazione socioeconomica.

> 💡 **Commento didattico**

Questo divieto incide direttamente sui sistemi di personalizzazione aggressiva (dark patterns cognitivi), sugli assistenti digitali per anziani progettati per indurre decisioni di acquisto, e su qualsiasi sistema che utilizzi dati psicografici per bypassare la razionalità decisionale. Il criterio discriminante è la volontà manipolativa: sistemi di nudging trasparente e consensuale rimangono consentiti.

b) Social scoring da parte di attori pubblici

È vietata la valutazione o la classificazione di persone fisiche da parte di autorità pubbliche — o per loro conto — sulla base di comportamenti sociali o caratteristiche personali o professionali, quando tale punteggio produce trattamento pregiudizievole in contesti diversi da quello in cui i dati sono stati raccolti, o trattamento sproporzionato rispetto ai comportamenti effettivi.

Commento didattico

Il riferimento esplicito è ai sistemi di «credito sociale» già implementati in alcuni Paesi. Per la PA italiana, questo divieto è particolarmente rilevante: qualsiasi sistema integrato di valutazione dei cittadini (es. scoring comportamentale per l'accesso ai servizi) deve essere attentamente esaminato per verificare che non realizzi indirettamente questa forma di classificazione.

c) Riconoscimento delle emozioni in ambiti sensibili

È vietato l'uso di sistemi di riconoscimento delle emozioni nei luoghi di lavoro e negli istituti di istruzione, salvo per finalità mediche o di sicurezza debitamente giustificate.

Commento didattico

Questa norma colpisce un'area in forte crescita commerciale: sistemi HR che analizzano le espressioni facciali durante i colloqui, piattaforme e-learning che monitorano l'attenzione degli studenti tramite webcam, strumenti di sorveglianza della produttività. La PA che adotta tali strumenti — o la software house che li propone — deve verificare con rigore la sussistenza di una deroga ammissibile.

d) Identificazione biometrica remota in tempo reale in spazi pubblici

È in linea di principio vietato l'uso di sistemi di identificazione biometrica remota in tempo reale in spazi accessibili al pubblico per finalità di contrasto. Sono ammesse deroghe strettamente circoscritte: ricerca di vittime di reati gravi, prevenzione di minacce terroristiche imminenti, individuazione di autori di reati specificamente elencati punibili con pena detentiva superiore a tre anni.

Commento didattico

Le deroghe richiedono autorizzazione giudiziaria preventiva (o, in caso di urgenza, ex post) e notifica all'autorità di vigilanza. Per i fornitori di sistemi di videosorveglianza intelligente destinati alla PA, questo è uno degli aspetti più critici: l'analisi biometrica offline (post-evento) è regolata come sistema ad alto rischio ma non è vietata.

e) Categorie biometriche e inferenza di caratteristiche sensibili

È vietato l'uso di sistemi AI che categorizzano biometricamente le persone per dedurre la razza, le opinioni politiche, le convinzioni religiose o filosofiche, l'orientamento sessuale, lo stato di salute — salvo specifiche deroghe per forze dell'ordine.

> **Commento didattico**
>
> Questo divieto si interseca profondamente con il GDPR, in particolare con l'articolo 9 sul trattamento delle categorie speciali di dati. L'AI Act introduce un divieto operativo che va oltre la mera limitazione del trattamento: vieta la progettazione stessa di sistemi con questa finalità inferenziale.

3. I sistemi AI ad alto rischio — Titolo III

Il cuore operativo del Regolamento per le software house che lavorano con la PA è il regime dell'alto rischio. I sistemi ad alto rischio non sono vietati, ma sono soggetti a un sistema di obblighi conformativi denso e articolato, il cui rispetto deve essere dimostrato prima della messa in servizio.

3.1 Cosa rende un sistema «ad alto rischio»

L'Allegato II individua sistemi AI embedded in prodotti già soggetti a legislazione settoriale di sicurezza (macchinari, dispositivi medici, veicoli autonomi, ecc.). L'Allegato III — di interesse primario per il contesto PA — elenca otto aree tematiche di alto rischio:

Area dell'Allegato III	Esempi applicativi per la PA
Infrastrutture critiche	Gestione reti idriche, energetiche, traffico con componenti AI
Istruzione e formazione professionale	Sistemi di valutazione automatizzata, selezione dei candidati a corsi pubblici
Occupazione e gestione HR	Screening dei CV per concorsi pubblici, valutazione delle performance
Accesso a servizi pubblici essenziali	Scoring per sussidi, indennità, prestazioni previdenziali, accesso ad alloggi sociali
Contrasto, giustizia e gestione delle frontiere	Profilazione predittiva, analisi rischio recidiva, sorveglianza delle frontiere
Migrazione e asilo	Valutazione automatizzata delle domande di protezione internazionale
Democrazia e istituzioni	Sistemi AI usati in procedure elettorali, applicazione della legge
Sicurezza pubblica	Riconoscimento facciale offline, analisi comportamentale in sorveglianza

⚠ Attenzione pratica

La Commissione Europea ha il potere di aggiornare l'Allegato III mediante atti delegati. Le software house devono quindi monitorare le evoluzioni normative in modo continuativo, poiché sistemi oggi classificati a rischio minimo potrebbero essere inseriti nell'elenco ad alto rischio in futuro.

3.2 Gli obblighi per i fornitori di sistemi ad alto rischio (Artt. 9–17)

Per ogni sistema AI classificato ad alto rischio, il fornitore deve adempiere a un insieme articolato di obblighi tecnici e documentali. Li analizziamo uno per uno, con commento applicativo.

a) Sistema di gestione del rischio (Art. 9)

Il fornitore deve istituire, documentare e mantenere un sistema di gestione del rischio per tutto il ciclo di vita del sistema AI. Questo non è un documento una-tantum: è un processo iterativo che comprende l'identificazione e l'analisi dei rischi noti e ragionevolmente prevedibili, la stima e la valutazione dei rischi residui, l'adozione di misure di gestione appropriate.

Commento

Il riferimento normativo è esplicito nel richiedere che le misure di gestione del rischio garantiscano un livello di rischio residuo accettabile in relazione allo stato dell'arte. Il sistema deve essere aggiornato ogni volta che il sistema AI viene aggiornato in modo significativo. Per il responsabile, questo significa integrare il risk management AI nel processo di sviluppo software (DevSecOps → DevSecAI).

b) Governance dei dati di addestramento (Art. 10)

I sistemi AI ad alto rischio che utilizzano tecniche di addestramento devono essere sviluppati con dataset che soddisfano criteri di qualità specifici: rilevanza, rappresentatività, libertà da errori per quanto fattibile, completezza rispetto alle finalità. È richiesta la gestione delle possibili distorsioni (bias) e la documentazione delle pratiche di governance dei dati.

Commento

Questo obbligo è particolarmente impegnativo per chi utilizza dataset della PA, spesso caratterizzati da lacune storiche, sottorappresentazione di categorie demografiche, o bias sistemici derivanti da prassi amministrative passate. La norma non richiede dati perfetti, ma impone un processo documentato di identificazione e mitigazione delle distorsioni — un requisito che incrocia direttamente le valutazioni di impatto GDPR (DPIA).

c) Documentazione tecnica (Art. 11 e Allegato IV)

Prima dell'immissione sul mercato, il fornitore deve redigere una documentazione tecnica completa. L'Allegato IV specifica il contenuto minimo: descrizione generale del sistema, specifiche tecniche, descrizione delle fasi di sviluppo, informazioni sulle prestazioni attese, descrizione delle capacità di monitoraggio.

Commento

La documentazione tecnica è il «fascicolo tecnico» dell'AI Act — equivalente a quanto già richiesto dalla normativa sui dispositivi medici o dalle direttive macchine. Deve essere tenuta aggiornata e messa a disposizione delle autorità di vigilanza su richiesta. Per le software house, questo impone un cambio culturale: la documentazione non è un adempimento formale post-sviluppo, ma deve accompagnare l'intero ciclo di vita.

d) Trasparenza e informazione agli utenti (Art. 13)

I sistemi ad alto rischio devono essere progettati in modo che il loro funzionamento sia sufficientemente trasparente da consentire ai deployer di interpretare gli output e utilizzarli in modo appropriato. Il fornitore deve fornire istruzioni per l'uso comprensibili, che includano: identità e contatti del fornitore, caratteristiche e limitazioni del sistema, livello di accuratezza atteso e possibili errori, misure di sorveglianza umana necessarie.

Commento

Il principio di trasparenza qui non riguarda solo la comunicazione verso il cittadino-utente finale, ma verso il deployer professionale (es. il funzionario della PA) che deve poter esercitare supervisione significativa sulle decisioni del sistema. Si tratta di un requisito di «explainability» operativa, non necessariamente algoritmica.

e) Supervisione umana (Art. 14)

I sistemi AI ad alto rischio devono essere progettati per poter essere efficacemente supervisionati da persone fisiche. Questo implica la progettazione di interfacce e strumenti che permettano ai supervisori umani di monitorare il funzionamento in tempo reale, comprendere le capacità e i limiti del sistema, intervenire o disattivare il sistema (funzione di «stop»), ignorare, sovrascrivere o ribaltare gli output.

Commento

Il principio di «human-in-the-loop» è un cardine dell'AI Act. Non è sufficiente che teoricamente un umano possa intervenire: il sistema deve essere progettato per rendere tale intervento pratico, tempestivo ed efficace. Nelle decisioni amministrative automatizzate che riguardano diritti soggettivi dei cittadini, questo requisito si sovrappone al diritto alla revisione umana garantito dall'Art. 22 GDPR.

f) Accuratezza, robustezza e cybersecurity (Art. 15)

Il sistema deve raggiungere un adeguato livello di accuratezza, robustezza e cybersecurity, secondo metriche documentate in fase di sviluppo. Particolare attenzione è richiesta alla resilienza rispetto a errori, guasti o manipolazioni (adversarial attacks). La norma richiede esplicitamente che vengano considerati i comportamenti del sistema in condizioni di errore.

Commento

Per le aziende già soggette a NIS2 (Direttiva sulla sicurezza delle reti e dei sistemi informativi), questo requisito si integra con gli obblighi di cybersecurity già vigenti. La robustezza include anche la stabilità degli output: un sistema AI che produce risultati erratici o non riproducibili — anche se mai «attaccato» — non soddisfa questo standard.

4. Obblighi specifici per deployer e ruoli della catena del valore

Il Regolamento introduce una chiara ripartizione di responsabilità lungo la catena del valore dei sistemi AI. Comprendere dove ci si posiziona è essenziale per identificare gli obblighi applicabili.

Ruolo	Definizione e obblighi principali
Fornitore (Provider)	Chi sviluppa e immette sul mercato il sistema AI. Porta gli obblighi più pesanti: conformità tecnica, documentazione, registrazione, dichiarazione di conformità, marcatura CE per prodotti regolati.
Deployer	Chi usa un sistema AI per uso professionale. Deve: applicare le istruzioni del fornitore; garantire supervisione umana; effettuare DPIA se richiesta dal GDPR; informare i lavoratori sull'uso di AI che li riguarda; segnalare incidenti gravi.
Importatore	Verifica che il fornitore esterno abbia assolto gli obblighi di conformità prima dell'immissione sul mercato UE.
Distributore	Verifica la presenza della documentazione di conformità prima della distribuzione. Responsabilità limitate ma non nulle.
Mandatario (Art. 22)	Persona fisica o giuridica stabilita nell'UE designata da fornitori extra-UE per agire per loro conto.

Il fornitore come deployer PA

Quando il fornitore che tratta dati per conto del titolare integra sistemi AI di terze parti (es. servizi cognitivi cloud, modelli foundation di grandi fornitori) nelle soluzioni destinate alla PA, assume il ruolo di deployer. Questo implica: verificare che il fornitore abbia assolto i suoi obblighi; adattare l'implementazione alle istruzioni d'uso; assicurare che la PA cliente abbia le informazioni necessarie per esercitare la supervisione umana; gestire eventuali segnalazioni di malfunzionamento.

5. Modelli di AI per finalità generali (GPAI) — Titolo VIII

Con il Titolo VIII, l'AI Act introduce un regime specifico per i modelli di AI per finalità generali (General Purpose AI — GPAI), ossia i large language models e i modelli fondazionali che

possono essere integrati in innumerevoli sistemi downstream. Questa è una delle parti più innovative e dibattute del Regolamento.

5.1 Definizione di modello GPAI

Un modello GPAI è un modello AI addestrato su grandi quantità di dati con metodi self-supervised, che mostra significativa generalizzabilità e che è in grado di svolgere competentemente un'ampia gamma di compiti distinti, potendo essere integrato in numerosi sistemi o applicazioni (Art. 3, par. 63).

5.2 Obblighi per i fornitori GPAI

Tutti i fornitori di modelli GPAI (art. 53) devono: redigere e mantenere documentazione tecnica; fornire informazioni e documentazione ai fornitori downstream; rispettare il diritto dell'Unione sul copyright, in particolare rendendo pubblica una sintesi dei contenuti di addestramento; pubblicare una politica di utilizzo accettabile.

> ⚠ **I modelli GPAI a rischio sistemico (Art. 51)**
>
> I modelli addestrati con una capacità di calcolo superiore a 10^25 FLOPs sono presunti a rischio sistemico e soggetti a obblighi aggiuntivi: valutazione delle capacità del modello, valutazione e mitigazione dei rischi sistemici, segnalazione di incidenti gravi all'UIEA, misure di cybersecurity adeguate. Questo regime riguarda attualmente un numero ristretto di grandi fornitori (OpenAI, Google DeepMind, Anthropic, Meta) ma potrebbe ampliarsi.

Per il responsabile al trattamento, la rilevanza principale è nella catena contrattuale: quando si integrano API di modelli GPAI (es. GPT-4, Gemini, Claude) in soluzioni per la PA, è necessario verificare che il fornitore del modello abbia rispettato i propri obblighi GPAI — in particolare la trasparenza sui dati di addestramento e la documentazione tecnica — e che ciò sia contrattualmente garantito.

6. Governance, vigilanza e sanzioni

Il Regolamento costruisce un'architettura di governance su due livelli: nazionale (Autorità nazionali di vigilanza) ed europeo (Ufficio per l'Intelligenza Artificiale — UIEA).

6.1 L'Ufficio per l'AI (UIEA)

Istituito in seno alla Commissione Europea, l'UIEA è il supervisore diretto dei fornitori di modelli GPAI e coordina l'applicazione uniforme del Regolamento. Pubblica linee guida, gestisce la banca dati europea dei sistemi AI ad alto rischio, gestisce le segnalazioni di incidenti gravi.

6.2 Le autorità nazionali

Ogni Stato membro deve designare almeno un'autorità nazionale competente entro agosto 2025. In Italia, il decreto-legge n. 19/2024 (convertito in legge) ha affidato provvisoriamente le funzioni all'Agenzia per l'Italia Digitale (AgID) in collaborazione con il Dipartimento per la trasformazione digitale, in attesa della designazione definitiva.

6.3 Il regime sanzionatorio (Art. 99–101)

Il Regolamento prevede sanzioni pecuniarie molto elevate, differenziate per tipologia di violazione e dimensione dell'impresa:

Tipo di violazione	Sanzione massima
Violazione dei divieti assoluti (Art. 5)	35.000.000 € o 7% del fatturato mondiale annuo (il maggiore)
Violazione degli obblighi per sistemi ad alto rischio	15.000.000 € o 3% del fatturato mondiale annuo
Informazioni false o fuorvianti alle autorità	7.500.000 € o 1,5% del fatturato mondiale annuo
Per PMI e startup	Sanzione non superiore al massimo previsto, con possibile riduzione

> ⚠ **Rilevanza per PMI**
>
> Il Regolamento prevede esplicitamente (Art. 99, par. 7) che le autorità nazionali tengano conto delle dimensioni aziendali, della natura, gravità e durata dell'infrazione, nonché del grado di cooperazione, nell'irrogazione delle sanzioni. Tuttavia, le soglie percentuali sul fatturato mondiale rendono le sanzioni potenzialmente significative anche per aziende di medie dimensioni.

7. Obblighi di trasparenza verso i cittadini (Art. 50)

L'Articolo 50 introduce obblighi di trasparenza specifici per tre categorie di sistemi che interagiscono direttamente con persone fisiche o producono contenuti sintetici:

a) Sistemi di interazione con persone fisiche (chatbot)

I deployer di sistemi AI progettati per interagire con persone fisiche devono informare queste ultime del fatto che stanno interagendo con un sistema AI, in modo chiaro e tempestivo, prima che l'interazione abbia inizio o al suo avvio. La norma non si applica se il contesto rende ovvia la natura artificiale del sistema (es. ovvio assistente vocale etichettato come tale).

> 💡 **Implicazione PA**

Tutti i chatbot istituzionali delle PA (assistenti virtuali per accesso ai servizi, bot di supporto ai cittadini) devono presentare un'etichetta chiara di AI. Non è sufficiente indicarlo solo nei termini di servizio o nella privacy policy.

b) Contenuti generati artificialmente (deepfake e synthetic media)

I sistemi AI che generano o manipolano immagini, audio o video con somiglianza a persone reali, eventi reali o luoghi reali devono assicurare che i contenuti siano marcati con disclosure della loro natura artificiale — in formato machine-readable e percepibile.

c) Riconoscimento delle emozioni e categorizzazione biometrica

Le persone fisiche esposte a sistemi di riconoscimento delle emozioni o di categorizzazione biometrica devono essere informate della loro esposizione, salvo specifiche eccezioni per le forze dell'ordine.

8. L'intersezione con il GDPR: un quadro composito

L'AI Act non è uno strumento isolato: opera in stretta sinergia — e a volte in tensione — con il Regolamento Generale sulla Protezione dei Dati (GDPR, Reg. UE 2016/679). Comprendere i punti di contatto è essenziale per costruire una compliance integrata.

Tema	AI Act
Governance dei dati	Art. 10: qualità, rappresentatività, bias dei dataset di addestramento
Supervisione umana	Art. 14: human oversight come requisito di progettazione
Trasparenza	Artt. 13, 50: trasparenza tecnica e verso utenti finali
Valutazione d'impatto	Art. 9: risk management per sistemi ad alto rischio
Accountability	Art. 17: sistema di gestione della qualità documentato
Diritti degli interessati	Normativa non specifica (ma complementare)

La DPIA come strumento di raccordo

In molti casi, la valutazione d'impatto sulla protezione dei dati (DPIA) prevista dal GDPR sarà lo strumento pratico per soddisfare contestualmente gli obblighi di risk management dell'AI Act. Le Linee Guida dell'EDPB suggeriscono che, per sistemi AI ad alto rischio che trattano dati personali, la DPIA debba essere arricchita con l'analisi specifica dei rischi AI (bias, opacità algoritmica, deriva dei modelli). Il fornitore dovrebbe sviluppare un template integrato DPIA+AI Risk Assessment.

9. Il calendario di applicazione

L'AI Act adotta un approccio di applicazione progressiva, con scadenze differenziate per tipologia di obbligo. Conoscere queste date è essenziale per la pianificazione della compliance aziendale.

Data	Obblighi in vigore
1° agosto 2024	Entrata in vigore del Regolamento
2 febbraio 2025	Applicazione dei divieti assoluti (Art. 5) — già in vigore. Designazione delle autorità nazionali competenti. Applicazione delle norme sulla governance e sanzioni GPAI.
2 agosto 2025	Applicazione degli obblighi per i fornitori GPAI (Titolo VIII). Applicazione delle norme su governance, responsabilità, riservatezza, sanzioni (Titoli III Capo 4, V, VII, IX-XIII).
2 agosto 2026	Piena applicazione per tutti i sistemi AI ad alto rischio dell'Allegato III (PA, occupazione, istruzione, ecc.). Applicazione dell'Art. 6 par. 1 per i prodotti regolati dall'Allegato II.
2 agosto 2027	Applicazione per i sistemi AI ad alto rischio incorporati in prodotti soggetti a legislazione settoriale preesistente (Allegato II) già immessi sul mercato.

Priorità immediata — febbraio 2025

I divieti assoluti dell'Art. 5 sono già pienamente applicabili. Ogni azienda dovrebbe aver già completato una mappatura dei propri sistemi AI per verificare che nessuno rientri nelle categorie vietate. Se questa analisi non è stata ancora eseguita, è la prima azione da intraprendere.

10. Roadmap di compliance per il Responsabile del trattamento

Sulla base dell'analisi normativa svolta, proponiamo una roadmap di compliance strutturata in fasi, calibrata sul profilo specifico di una software house che opera nel settore pubblico.

Fase 1 — Mappatura e classificazione (entro 60 giorni)

1. Inventario dei sistemi AI: censimento di tutti i sistemi AI sviluppati, commercializzati o integrati dal fornitore, con indicazione della versione, del mercato di riferimento e della funzionalità principale.
2. Classificazione del rischio: per ciascun sistema, verifica dell'applicabilità dell'Art. 5 (divieti) e degli Allegati II e III (alto rischio), nonché del regime GPAI se rilevante.
3. Mappatura dei ruoli: identificazione del ruolo(fornitore, deployer, o entrambi) per ciascun sistema censito.

Fase 2 — Gap analysis e prioritizzazione (30-90 giorni)

4. Per i sistemi ad alto rischio: analisi delle lacune documentali rispetto ai requisiti degli Artt. 9-17.
5. Valutazione delle procedure esistenti di governance dei dati, risk management e cybersecurity, con identificazione delle integrazioni necessarie.
6. Verifica contrattuale dei fornitori di sistemi AI e modelli GPAI integrati nelle soluzioni fornite.

Fase 3 — Adeguamento tecnico e documentale (90-180 giorni)

7. Sviluppo di template documentali standard: fascicolo tecnico, istruzioni per l'uso, dichiarazione di conformità.
8. Integrazione del risk management AI nel processo di sviluppo software aziendale.
9. Sviluppo di un template integrato DPIA + AI Risk Assessment per le soluzioni destinate alla PA.
10. Formazione del personale tecnico e dei project manager sui requisiti dell'AI Act.

Fase 4 — Monitoring e aggiornamento continuo

11. Istituzione di un presidio interno di monitoraggio normativo (AI compliance officer o team dedicato).
12. Definizione di procedure di incident reporting per i sistemi ad alto rischio.
13. Pianificazione delle revisioni periodiche della documentazione tecnica in caso di aggiornamenti significativi dei sistemi.

Conclusioni — L'AI Act come opportunità strategica

Sarebbe un errore strategico considerare l'AI Act esclusivamente come un onere normativo. Per una software house la compliance diventa un asset competitivo nei confronti della pubblica amministrazione: una PA che adotta sistemi AI ha precisi obblighi di verifica nei confronti dei propri fornitori, e un fornitore documentalmente conforme ha un vantaggio di posizionamento significativo nelle gare pubbliche.

L'Unione Europea sta costruendo, con l'AI Act, il GDPR e la NIS2, un ecosistema normativo coerente e internazionalmente riconoscibile per la governance del digitale. Le aziende che anticipano questi requisiti, integrandoli nella propria cultura di sviluppo, non subiscono la regolamentazione: la utilizzano come differenziatore.

Messaggio finale

La domanda non è «se» l'AI Act si applica al fornitore, ma «come» prepararsi in modo intelligente, progressivo e valorizzante. La compliance non è la fine dell'innovazione: è la condizione per un'innovazione sostenibile, fiduciaria e scalabile nel mercato europeo.

Riferimenti normativi e documentali

- Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 (AI Act) — GUUE L 2024/1689 del 12.7.2024
- Regolamento (UE) 2016/679 (GDPR) — GUUE L 119/1 del 4.5.2016
- Direttiva (UE) 2022/2555 (NIS2) — GUUE L 333 del 27.12.2022
- Linee Guida EDPB n. 05/2020 — Decisioni automatizzate e profilazione
- Linee Guida ENISA — AI Cybersecurity, ottobre 2023
- Decreto-legge 2 marzo 2024, n. 19 (convertito in L. 29 aprile 2024, n. 56) — Disposizioni nazionali attuative
- UIEA — Linee guida per i fornitori di sistemi AI ad alto rischio, 2024
- AgID — Linee Guida sull'acquisizione di software nella PA (aggiornamento 2024)