AGID academy

AGID | Agenzia per l'Italia Digitale

AI ACT, NEW LEGISLATIVE FRAMEWORK E STANDARD ARMONIZZATI

Sintesi

Gennaio 2026

Sommario

Abstract e avvertenze

Il presente documento costituisce una sintesi introduttiva all'inquadramento dell'AI Act nel contesto del NLF, con particolare riferimento al ruolo degli standard armonizzati nel sistema europeo di regolazione dei prodotti. L'obiettivo, senza l'ambizione di fornire una trattazione esaustiva dell'AI Act, del New Legislative Framework (NLF) e del sistema degli standard armonizzati, è invece quello di introdurre alcuni concetti fondamentali utili a comprendere le logiche, i ruoli e i principali meccanismi che disciplinano l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di intelligenza artificiale nell'Unione europea.

Il documento richiama in forma sintetica l'impianto regolatorio europeo, l'approccio basato sul rischio e il principio della presunzione di conformità, nonché la classificazione dei sistemi di IA, con focus sui sistemi ad alto rischio. Sono inoltre delineati i ruoli e gli obblighi di fornitori e deployer, i principali requisiti tecnici e organizzativi e le procedure di valutazione della conformità, con un cenno allo stato di avanzamento degli standard armonizzati.

Le indicazioni contenute nel presente testo hanno finalità esclusivamente informative e orientative. Una trattazione più estensiva e sistematica dei temi affrontati, nonché degli ulteriori approfondimenti sviluppati nel corso del webinar, sarà oggetto di successivi documenti e contributi dedicati.

Resta in ogni caso imprescindibile il riferimento diretto al testo ufficiale del Regolamento (UE) 2024/1689 e agli atti attuativi e tecnici collegati, quale fonte primaria per l'interpretazione e l'applicazione delle relative disposizioni normative.

Introduzione e contesto

L'ecosistema normativo europeo relativo all'intelligenza artificiale è in rapida evoluzione. Attraverso regole comuni, standard condivisi e interoperabilità, l'Unione europea mira a costruire un quadro regolatorio nel quale innovazione, sicurezza e tutela dei diritti fondamentali procedano congiuntamente, favorendo la crescita e la competitività di cittadini, imprese e pubbliche amministrazioni.

L'UE stabilisce requisiti rigorosi per i beni e i servizi che accedono al proprio mercato. Tali regole, per effetto della rilevanza economica del mercato europeo, vengono spesso adottate anche al di fuori dell'Unione da parte delle grandi imprese globali che adeguano i propri prodotti agli standard europei per continuare a operare nel mercato interno, generando un impatto regolatorio su scala internazionale (cd. *Brussels Effect*).

In questo contesto, l'AI Act rappresenta la prima regolazione organica e orizzontale dell'intelligenza artificiale nell'Unione europea, in coerenza con altre normative dell'UE, in particolare in materia di vigilanza del mercato e sicurezza dei prodotti. Il regolamento si inserisce nel solco del New Legislative Framework (NLF), un impianto normativo già consolidato e utilizzato per la disciplina di prodotti quali macchine, dispositivi medici, apparecchiature di sicurezza e giocattoli.

L'AI Act adotta e adatta tale schema alla specificità dei sistemi di IA, con l'obiettivo di garantire che i sistemi immessi sul mercato europeo rispettino elevati standard di sicurezza, affidabilità e tutela dei diritti fondamentali, rafforzando al contempo la fiducia e la trasparenza nel mercato unico digitale.

Il New Legislative Framework (NLF) in breve

Il New Legislative Framework (NLF) rappresenta l'architettura regolatoria che definisce, a livello dell'Unione europea, le modalità con cui i prodotti regolamentati devono essere

progettati, verificati, controllati e immessi sul mercato. Tale impianto si fonda su tre elementi essenziali:

1. requisiti legali essenziali stabiliti dalla normativa europea;
2. standard tecnici armonizzati che traducono tali requisiti in specifiche tecniche verificabili;
3. procedure di valutazione della conformità, che possono essere svolte internamente dal fabbricante/fornitore oppure da organismi notificati indipendenti.

Quando un operatore economico applica correttamente gli standard armonizzati pertinenti, pubblicati nella Gazzetta Ufficiale dell'Unione europea, beneficia della presunzione di conformità ai corrispondenti requisiti legali. Tale meccanismo semplifica la dimostrazione della conformità e facilita l'accesso al mercato unico.

Questo stesso schema è adottato dall'AI Act: i requisiti specifici per i sistemi di intelligenza artificiale si innestano nel consolidato impianto del NLF, assicurando coerenza tra i diversi settori regolati e certezza giuridica per gli operatori economici.

L'AI Act e la logica basata sul rischio

Il Regolamento (UE) 2024/1689 sull'intelligenza artificiale costituisce il primo quadro normativo organico e orizzontale in materia di IA. Esso si compone di 113 articoli, suddivisi in XIII capi, e di XIII allegati. L'AI Act disciplina l'intero ciclo di vita dei sistemi di intelligenza artificiale, dalla progettazione e sviluppo, alla messa in servizio e all'uso, fino alle attività di monitoraggio post-market.

Il regolamento adotta un approccio basato sul rischio (*risk-based approach*), distinguendo tra diverse categorie di rischio:

- **rischio inaccettabile**, che comprende pratiche vietate in quanto intrinsecamente lesive dei diritti fondamentali;
- **alto rischio**, che ricomprende i sistemi soggetti ai requisiti più stringenti;
- **rischio limitato**, per i quali si applicano principalmente obblighi di trasparenza e informazione;
- **rischio minimo**, per cui non sono previsti obblighi specifici ai sensi dell'AI Act.

Le pratiche vietate includono, tra l'altro, taluni impieghi di sistemi biometrici in tempo reale in spazi pubblici, salvo specifiche deroghe previste dalla legge. La categoria dell'alto rischio, oggetto principale della disciplina regolatoria, riguarda sia i sistemi che costituiscono componenti di sicurezza di prodotti già regolati dalla normativa europea (Allegato I), sia le nuove categorie individuate nell'Allegato III, tra cui biometria, infrastrutture critiche, istruzione e formazione, occupazione, accesso a servizi essenziali, attività di law enforcement, migrazione e asilo, amministrazione della giustizia e processi democratici.

Il regolamento opera una chiara distinzione tra modelli di IA per finalità generali (GPAI) e sistemi di IA ad alto rischio.

I modelli generativi, in particolare, sono tenuti a rispettare obblighi orizzontali di trasparenza, documentazione tecnica e sicurezza e, per quelli che presentano un rischio sistemico, sono previsti requisiti rafforzati. In questa fase di prima applicazione del regolamento, in attesa dell'adozione degli standard armonizzati e di ulteriori specificazioni tecniche dedicate, un ruolo di accompagnamento è svolto dal Code of Practice per i GPAI, cui i produttori possono aderire su base volontaria quale strumento di supporto alla conformità.

Sistemi ad alto rischi (Allegato I e Allegato III)

L'AI Act individua due distinti percorsi per la qualificazione e la disciplina dei sistemi di IA ad alto rischio.

Nel primo caso (Allegato I), l'IA costituisce componente di sicurezza di prodotti già regolati da normative armonizzate dell'Unione europea (ad esempio dispositivi medici, macchine, droni). In tali ipotesi, i requisiti previsti dall'AI Act si integrano nella procedura di valutazione della conformità prevista dalla normativa settoriale applicabile. Prevale la procedura più stringente e l'organismo notificato competente per il settore specifico, ove debitamente qualificato, può estendere la propria verifica anche ai requisiti stabiliti dall'AI Act.

Nel secondo caso (Allegato III), il regolamento individua categorie autonome di sistemi di IA considerati ad alto rischio, tra cui: biometria, gestione di infrastrutture critiche, istruzione e valutazione delle competenze, occupazione e gestione del lavoro, accesso a servizi essenziali pubblici e privati, attività di law enforcement, gestione della migrazione, asilo e controllo delle frontiere, amministrazione della giustizia e processi democratici. Per tali sistemi, la valutazione della conformità segue le procedure previste dagli allegati specifici dell'AI Act, che possono consistere in un controllo interno del fornitore oppure nell'intervento di un organismo notificato, a seconda dei casi previsti dal regolamento.

Requisiti per i sistemi di IA ad alto rischio

I sistemi di IA ad alto rischio sono soggetti a requisiti articolati e proporzionati al contesto d'uso e ai rischi generati per salute, sicurezza e diritti fondamentali.

Tra i principali obblighi previsti dal regolamento figurano:

- **Risk Management System (art. 9)**: processo continuo lungo l'intero ciclo di vita del sistema, comprendente identificazione, analisi, mitigazione e rivalutazione dei rischi per salute, sicurezza e diritti fondamentali, incluso l'uso improprio ragionevolmente prevedibile.

- **Data governance (art. 10)**: requisiti di qualità dei dati di training, validation e testing, con attenzione a provenienza, rappresentatività, riduzione dei bias, documentazione delle trasformazioni e delle ipotesi sottostanti. L'uso di categorie particolari di dati personali è ammesso solo in casi eccezionali, quando strettamente necessario e con garanzie rafforzate.

- **Logging e tracciabilità (art. 12)**: predisposizione di registrazioni automatiche adeguate a supportare audit, sicurezza e monitoraggio post-market, con requisiti specifici per determinate applicazioni, quali i sistemi biometrici.

- **Trasparenza e istruzioni d'uso (art. 13)**: fornitura di informazioni chiare e comprensibili sulle capacità e i limiti del sistema, sulle prestazioni attese, sulle condizioni d'uso e sulle misure di supervisione umana previste.

- **Supervisione umana (art. 14)**: garanzia di un controllo umano effettivo, prevenzione dell'automation bias e possibilità di ignorare, annullare o interrompere in sicurezza gli output del sistema.

- **Accuratezza, robustezza e cybersecurity (art. 15)**: definizione e comunicazione di metriche di prestazione, coerenza delle performance nel tempo, resilienza rispetto a errori e attacchi (ad esempio data poisoning, model poisoning e attacchi adversarial), con misure proporzionate al livello di rischio.

Ruoli: fornitore e deployer

Il **fornitore** (provider), ossia il soggetto che sviluppa o fa sviluppare e immette sul mercato o mette in servizio un sistema di IA a proprio nome o marchio, è destinatario di obblighi estesi in materia di progettazione, documentazione tecnica, testing, controllo qualità e monitoraggio post-market.

In particolare, il fornitore deve adottare un **Quality Management System (art. 17)** che copra l'intero ciclo di vita del sistema, inclusi progettazione, sviluppo, gestione dei dati, risk management, monitoraggio post-market e gestione degli incidenti, assicurando responsabilità organizzative chiare e proporzionalità rispetto alla dimensione e complessità dell'organizzazione.

Il **deployer**, ossia il soggetto che utilizza il sistema sotto la propria autorità, è tenuto a garantire un uso corretto e responsabile del sistema, nel rispetto delle istruzioni fornite dal produttore e delle condizioni previste dal regolamento. Tra gli obblighi rilevanti rientra, ove richiesto, la valutazione d'impatto sui diritti fondamentali (Fundamental Rights Impact Assessment, FRIA) e la cooperazione con le autorità competenti.

Valutazione di conformità e marcatura CE

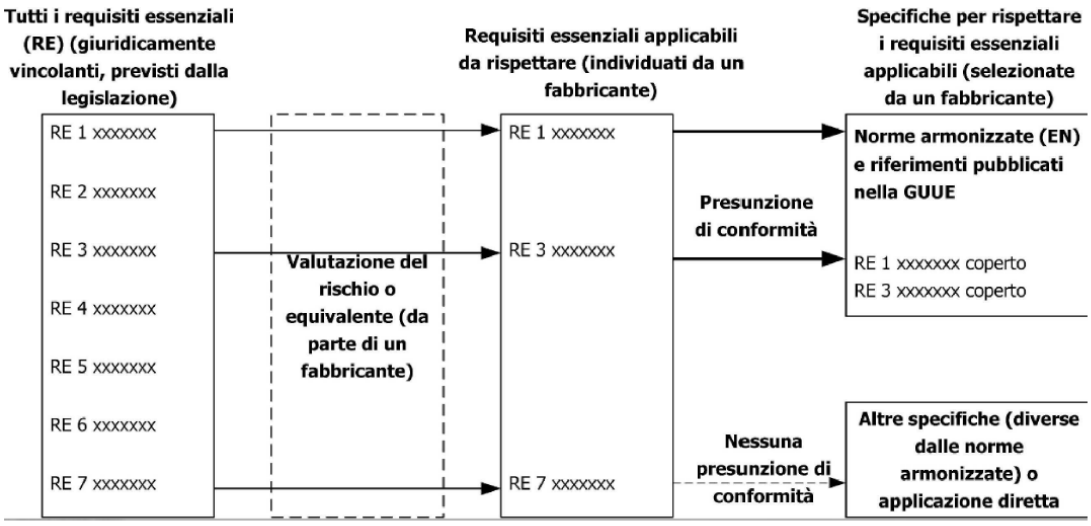
La conformità dei sistemi di IA ad alto rischio può essere valutata mediante controllo interno del fornitore oppure, nei casi previsti dal regolamento, con l'intervento di una terza parte indipendente (organismo notificato). Quest'ultima modalità si applica, in particolare, a taluni sistemi biometrici o quando richiesto dalla normativa settoriale applicabile ai sensi dell'Allegato I.

Il processo di valutazione culmina, in caso di esito positivo, con la redazione della dichiarazione UE di conformità e l'apposizione della marcatura CE, che consente l'immissione sul mercato o la messa in servizio del sistema nell'Unione europea. In caso di

esito negativo, il fornitore è tenuto ad adottare le necessarie azioni correttive prima di procedere a una nuova verifica.

La valutazione di conformità non costituisce un mero adempimento formale, ma un'attività sostanziale volta a verificare l'adeguatezza del sistema rispetto ai rischi identificati e ai requisiti normativi applicabili. Quando interviene un organismo notificato, sono previsti meccanismi di sorveglianza e controlli nel tempo, a garanzia del mantenimento della conformità.

Figura 1 – NLF e presunzione di conformità



Fonte: 'Blue Guide' on the implementation of EU product rules 2022. EC Commissione notice 2022/C 247/01.

Lo schema rappresenta il funzionamento del New Legislative Framework: dai requisiti essenziali stabiliti dalla normativa europea, il fabbricante individua quelli applicabili al proprio prodotto mediante una valutazione del rischio. L'applicazione delle norme armonizzate pubblicate in Gazzetta Ufficiale dell'Unione europea consente di beneficiare della presunzione di conformità ai corrispondenti requisiti; in assenza di norme armonizzate pertinenti, il rispetto dei requisiti deve essere dimostrato mediante altre specifiche tecniche o tramite applicazione diretta della normativa.

Standard armonizzati e governance

Gli standard armonizzati sono elaborati dagli enti europei di normazione (CEN e CENELEC, ed ETSI) su richiesta formale della Commissione europea (*standardisation request*). Per l'AI Act, la richiesta di normazione copre i principali ambiti tecnici del regolamento, tra cui: terminologia, sistemi di gestione del rischio (RMS), sistemi di gestione della qualità (QMS), data governance, logging e tracciabilità, trasparenza, supervisione umana, accuratezza, robustezza e cybersecurity, nonché aspetti connessi alla valutazione della conformità.

Gli standard armonizzati costituiscono l'infrastruttura tecnica su cui si fonda il meccanismo della presunzione di conformità. Una volta pubblicati nella Gazzetta Ufficiale dell'Unione europea, essi consentono agli operatori economici di dimostrare il rispetto dei requisiti legali corrispondenti.

In assenza temporanea di standard armonizzati, la Commissione può adottare specifiche comuni, al fine di preservare il funzionamento del sistema di conformità e garantire un livello uniforme di applicazione del regolamento. I lavori di normazione procedono con tempistiche differenziate e hanno registrato alcuni ritardi. In tale contesto, il cosiddetto Digital Omnibus, attualmente in corso di definizione, prevede una dilazione dei termini di applicazione di taluni obblighi relativi ai sistemi di IA ad alto rischio, al fine di consentire agli enti europei di normazione di completare l'elaborazione degli standard armonizzati.

Alla data di redazione del presente report, il Digital Omnibus prevede le seguenti scadenze:

- 2 dicembre 2027 – Sistemi di IA rientranti nell'Allegato I (IA integrata in prodotti già regolati da normativa settoriale);
- 2 agosto 2028 – Sistemi di IA rientranti nell'Allegato III (categorie autonome di sistemi ad alto rischio).

Tali tempistiche sono funzionali a garantire un'applicazione graduale e coordinata del regolamento, in coerenza con la disponibilità degli standard tecnici necessari a supportare il meccanismo della presunzione di conformità.

Governance dell'AI Act

La governance dell'AI Act si articola su più livelli istituzionali.

A livello europeo operano:

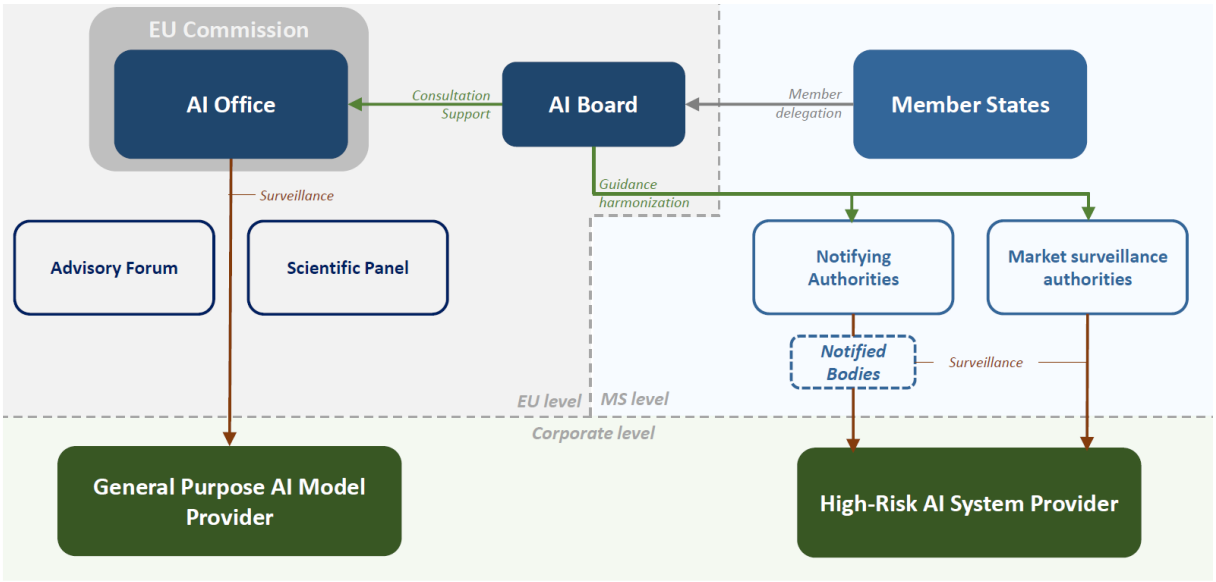
- l'AI Office, istituito presso la Commissione europea, con compiti di coordinamento e supervisione, in particolare per i modelli di IA per finalità generali;
- l'AI Board, composto dai rappresentanti degli Stati membri, con funzioni di supporto e coordinamento nell'attuazione del regolamento.

A livello nazionale sono previste:

- le autorità di sorveglianza del mercato, competenti per il controllo della conformità dei sistemi immessi sul mercato o messi in servizio;
- le autorità di notifica, responsabili della designazione e della vigilanza sugli organismi notificati incaricati delle valutazioni di conformità.

Tale assetto multilivello è finalizzato ad assicurare coordinamento, uniformità applicativa e coerenza nell'attuazione del regolamento all'interno del mercato unico.

Figura 2 - Implementazione dell'IA Act: compiti di EC e Stati Membri



Checklist operative

Le checklist che seguono sono fornite a titolo meramente esemplificativo e non hanno carattere esaustivo. Esse sintetizzano alcuni dei principali adempimenti previsti dall'AI Act con finalità orientativa e divulgativa.

L'effettiva applicazione degli obblighi richiede una valutazione caso per caso, alla luce delle specifiche caratteristiche del sistema di IA, del contesto di utilizzo, del settore di riferimento e dell'eventuale normativa settoriale applicabile.

Resta ferma la necessità di un'analisi giuridica e tecnica puntuale ai fini della piena conformità al regolamento e agli atti attuativi, inclusi gli standard armonizzati e le eventuali specifiche comuni adottate dalla Commissione europea.

A. Checklist per il Fornitore (Provider)

Le checklist che seguono sono fornite a titolo meramente esemplificativo e non hanno carattere esaustivo. Esse sintetizzano alcuni dei principali adempimenti previsti dall'AI Act con finalità orientativa e divulgativa.

L’effettiva applicazione degli obblighi richiede una valutazione caso per caso, alla luce delle specifiche caratteristiche del sistema di IA, del contesto di utilizzo, del settore di riferimento e dell’eventuale normativa settoriale applicabile.

Resta ferma la necessità di un’analisi giuridica e tecnica puntuale ai fini della piena conformità al regolamento e agli atti attuativi, inclusi gli standard armonizzati e le eventuali specifiche comuni adottate dalla Commissione europea.

1. Qualificazione del sistema

- Verificare se il sistema rientra tra le pratiche vietate
- Valutare se il sistema è classificabile come **alto rischio (Allegato I o III)**
- Verificare se si tratta di un modello GPAI o di un sistema specifico

2. Risk Management System (art. 9)

- Implementare un processo continuo di identificazione, analisi e mitigazione dei rischi
- Considerare l’uso improprio ragionevolmente prevedibile
- Documentare le valutazioni e le misure adottate

3. Data governance (art. 10)

- Verificare qualità, provenienza e rappresentatività dei dataset
- Valutare e mitigare bias sistematici
- Documentare trasformazioni e ipotesi metodologiche
- Garantire conformità alla normativa privacy

4. Requisiti tecnici

- Logging e tracciabilità adeguati
- Istruzioni d’uso chiare e complete

- Supervisione umana effettiva
- Metriche di accuratezza dichiarate
- Misure di robustezza e cybersecurity proporzionate al rischio

5. Quality Management System (art. 17)

- Integrare RMS, gestione dati e controllo qualità
- Definire responsabilità organizzative
- Prevedere procedure di gestione incidenti e post-market monitoring

6. Valutazione di conformità

- Determinare la procedura applicabile (controllo interno o organismo notificato)
- Redigere la documentazione tecnica
- Predisporre la dichiarazione UE di conformità
- Apporre la marcatura CE

7. Post-market monitoring

- Attivare sistemi di monitoraggio continuo
- Segnalare incidenti gravi alle autorità competenti
- Aggiornare la valutazione del rischio se necessario

B. Checklist per il Deployer

1. Verifica preliminare

- Accertare che il sistema rechi marcatura CE (se alto rischio)
- Verificare la documentazione fornita dal provider

2. Uso responsabile

- Utilizzare il sistema conformemente alle istruzioni

- Garantire adeguata supervisione umana
- Prevenire usi impropri

3. Valutazione d'impatto (se prevista)

- Effettuare la valutazione d'impatto sui diritti fondamentali
- Integrare la valutazione con eventuale DPIA (privacy)

4. Monitoraggio e segnalazione

- Monitorare prestazioni e anomalie
- Segnalare incidenti o malfunzionamenti al fornitore e alle autorità

Conclusioni

L'AI Act inserisce i sistemi di intelligenza artificiale nel consolidato meccanismo del New Legislative Framework, spostando l'attenzione dal "se" adottare l'IA al "come" farlo in modo affidabile, sicuro e conforme al diritto dell'Unione. Per gli operatori economici e le pubbliche amministrazioni, la priorità è dotarsi di adeguati processi di gestione del rischio e della qualità, di una governance dei dati solida e verificabile e di una documentazione tecnica strutturata, valutando tempestivamente la necessità di ricorrere a organismi notificati e monitorando l'evoluzione degli standard armonizzati.

L'AI Act rappresenta un punto di svolta per l'ecosistema digitale europeo. La sua attuazione richiede consapevolezza normativa, capacità organizzativa e preparazione tecnica. La combinazione tra NLF, requisiti sostanziali, standard armonizzati e meccanismi di valutazione della conformità costituisce l'architettura attraverso cui l'Unione europea intende garantire un utilizzo dell'intelligenza artificiale affidabile, sicuro e rispettoso dei diritti fondamentali nel mercato unico.

Glossario

AI Act: Regolamento (UE) 2024/1689 sull'Intelligenza Artificiale.

NLF (New Legislative Framework): impianto UE per l'armonizzazione tecnica e la presunzione di conformità.

Presunzione di conformità: effetto per cui l'applicazione di norme armonizzate pubblicate in GUUE consente di ritenere soddisfatti i requisiti corrispondenti.

Sistema ad alto rischio: sistema di IA che rientra nelle condizioni dell'art. 6 (Allegato I o Allegato III) e soggetto ai requisiti della Sezione 2.

RMS (Risk Management System): sistema di gestione del rischio lungo il ciclo di vita del sistema (art. 9).

QMS (Quality Management System): sistema di gestione della qualità del fornitore per assicurare conformità (art. 17).

Organismo notificato: soggetto terzo designato dall'autorità di notifica, competente per valutazioni di conformità quando previste.

AI Office / AI Board: organi europei di coordinamento e indirizzo per l'attuazione dell'AI Act.

Digital Omnibus: pacchetto legislativo che introduce flessibilità temporali legate alla disponibilità degli standard.