STRATEGIC POLICY BRIEF

AI Act dopo il Digital Omnibus

Obblighi applicabili, nuove scadenze e priorità di governance per provider e deployer

3 agosto 2026

MESSAGGIO CHIAVE

Il rinvio di una parte del regime high-risk non sospende l'AI Act. Dal 2 agosto 2026 il tema non è più soltanto comprendere la norma, ma dimostrare che ruoli, controlli e responsabilità sono effettivamente governati.

Il Regolamento (UE) 2026/1744, noto come Digital Omnibus on AI, ha modificato il calendario e alcune disposizioni dell'AI Act. Ha concesso più tempo per una parte degli obblighi relativi ai sistemi ad alto rischio, ma non ha sostituito l'AI Act né ha creato una moratoria generale. Il quadro applicabile nasce oggi dalla lettura coordinata del Regolamento (UE) 2024/1689 e delle modifiche entrate in vigore il 27 luglio 2026.

Per le organizzazioni, la conseguenza è rilevante: una data rinviata non elimina gli obblighi già operativi, quelli che acquistano efficacia il 2 agosto 2026 o la necessità di preparare per tempo sistemi che resteranno in esercizio negli anni successivi. Questo brief ricostruisce il calendario e traduce le principali disposizioni in decisioni di governance.

1. Il punto di partenza: il rinvio è selettivo

La modifica più visibile riguarda le Sezioni 1, 2 e 3 del Capo III dell'AI Act, che comprendono la classificazione dei sistemi ad alto rischio, i requisiti applicabili a tali sistemi e gli obblighi degli operatori. Fatta eccezione per l'articolo 6, paragrafo 5, tali disposizioni si applicheranno:

- dal **2 dicembre 2027**, per i sistemi classificati ad alto rischio ai sensi dell'articolo 6, paragrafo 2, e dell'Allegato III;
- dal **2 agosto 2028**, per i sistemi classificati ad alto rischio ai sensi dell'articolo 6, paragrafo 1, in collegamento con l'Allegato I.

Sono quindi posticipati, per queste categorie, i requisiti su gestione del rischio, governance dei dati, documentazione tecnica, registrazione automatica degli eventi, supervisione umana, accuratezza, robustezza e cybersicurezza, insieme ai correlati obblighi di provider, deployer e altri operatori.

LA DISTINZIONE DA NON PERDERE

Sono rinviate specifiche disposizioni del regime high-risk. Non sono rinviati l'intero AI Act, gli obblighi già applicabili, le regole di trasparenza né il rafforzamento dell'enforcement.

Perché il quadro è più complesso, non semplicemente più lungo

L'organizzazione non può fermarsi alla domanda "quando si applica l'AI Act?". Deve determinare, per ogni soluzione e caso d'uso, quale ruolo assume nella catena del valore, quale disposizione è rilevante, quale regime transitorio opera e quali evidenze dovranno essere disponibili. Le scadenze sono diverse e dipendono dalla natura del sistema, dalla data di immissione sul mercato o messa in servizio, dall'eventuale modifica del design e dal soggetto che lo utilizza.

Il calendario è dunque un problema di portafoglio e non soltanto un problema legale: sistemi diversi, anche all'interno della stessa impresa, possono seguire percorsi di adeguamento differenti.

2. Che cosa cambia dal 2 agosto 2026

Il **2 agosto 2026** resta una data cruciale: diventano applicabili gli obblighi di trasparenza dell'articolo 50, la nuova disciplina dell'articolo 4-bis sul trattamento di categorie particolari di dati per l'individuazione e la correzione dei bias e le sanzioni previste (articolo 101) per alcune violazioni dei provider di modelli di IA per finalità generali. Si rafforza inoltre l'attività di vigilanza dell'AI Office e delle autorità nazionali.

3. Trasparenza: dall'interfaccia alla prova di conformità

L'articolo 50 distribuisce obblighi distinti tra provider e deployer. La trasparenza non coincide con l'inserimento di una formula standard: richiede di comprendere chi progetta il sistema, chi lo mette a disposizione, chi lo utilizza e quale persona è esposta all'interazione o al contenuto.

Obblighi dei provider

- I sistemi destinati a interagire direttamente con *persone* devono informare l'interessato che sta interagendo con un sistema di AI, salvo che ciò risulti evidente a una persona ragionevolmente informata, attenta e avveduta nel contesto considerato. L'informazione deve essere chiara, distinguibile, accessibile e fornita entro la prima interazione.
- I sistemi che generano *audio, immagini, video* o *testi* sintetici devono produrre output contrassegnati in formato leggibile da macchina e rilevabili come artificialmente generati o manipolati, nei limiti e con le eccezioni previste dall'articolo 50.

AI agentica: un punto cieco da presidiare

L'AI Act non prevede una categoria giuridica autonoma per i sistemi agentici, ma questo non li esclude dal perimetro regolatorio. Due punti meritano attenzione immediata:

- se l'agente interagisce direttamente con una persona, ricade negli obblighi di trasparenza dell'art. 50 come qualsiasi altro sistema interattivo;
- le bozze di linee guida della Commissione sulla classificazione high-risk (19 maggio 2026) chiariscono che i sistemi agentici complessi vanno valutati nel loro insieme: un singolo

componente apparentemente marginale può comunque risultare ad alto rischio se contribuisce a un output rilevante ai sensi dell'Allegato III.

DECISIONE DI GOVERNANCE

Prima di delegare compiti operativi a un agente AI, l'organizzazione dovrebbe definire chi autorizza l'agente ad agire, entro quali limiti, con quale tracciabilità delle azioni intraprese e chi risponde in caso di errore o danno indipendentemente dal fatto che il singolo componente tecnico sia o meno, isolatamente, ad alto rischio.

Per i sistemi già immessi sul mercato prima del 2 agosto 2026, la sola obbligazione relativa al contrassegno e alla rilevabilità di cui all'articolo 50, paragrafo 2, beneficia di un periodo transitorio fino al 2 dicembre 2026.

La Commissione ha chiarito, nelle proprie linee guida del 20 luglio 2026, che l'esenzione basata sull'"ovvietà" dell'interazione con un sistema di AI va interpretata restrittivamente. I provider che intendono avvalersene devono poter giustificare e documentare la valutazione compiuta: non basta ritenere l'interazione ovvia, occorre poterlo dimostrare in caso di controllo.

Obbligo provider	Cosa deve garantire il provider	Tempistica
Disclosure dell' interazione AI-persona	Informare l'utente, in modo chiaro, distinguibile e accessibile, che sta interagendo con un sistema di AI, salvo ovvietà (da interpretare restrittivamente)	Entro la prima interazione
Marcatura dei contenuti generati	Contrassegnare audio, immagini, video e testo sintetici in formato leggibile da macchina e rilevabile	Dal 2 agosto 2026; fino al 2 dicembre 2026 per sistemi già sul mercato
Evidenza a supporto della conformità	Conservare documentazione tecnica, attività di validazione e registri a supporto della conformità	Continuativa

Obblighi dei deployer

- **Informare** le persone esposte all'uso di sistemi di riconoscimento delle emozioni o categorizzazione biometrica, quando l'impiego sia altrimenti lecito e fermo restando il diritto della protezione dei dati.
- **Dichiarare** che immagini, audio o video qualificabili come deepfake sono stati generati o manipolati artificialmente, tenendo conto delle regole specifiche per opere artistiche, creative, satiriche o analoghe.
- **Dichiarare** la generazione o manipolazione artificiale di testi pubblicati per informare il pubblico su questioni di interesse pubblico, salvo il caso di effettivo controllo umano o editoriale e di responsabilità editoriale in capo a una persona fisica o giuridica.

Obbligo del deployer	Cosa deve garantire il deployer	Tempistica
Riconoscimento delle emozioni e categorizzazione biometrica	Informare le persone esposte all'uso del sistema, quando l'impiego sia altrimenti lecito	Entro la prima esposizione
Deepfake	Dichiarare che il contenuto (immagine, audio, video) è stato generato o manipolato artificialmente, salvo eccezioni per opere artistiche/satiriche/creative	In modo chiaro e distinguibile, al più tardi al momento della prima esposizione al contenuto
Testi su questioni di interesse pubblico	Dichiarare la generazione/manipolazione artificiale del testo, salvo controllo editoriale umano con responsabilità di una persona fisica o giuridica	Entro la prima esposizione

IMPLICAZIONE MANAGERIALE

Il marking tecnico del provider e la comunicazione visibile del deployer sono controlli differenti. Contratti, procurement, comunicazione e gestione del prodotto devono attribuirli senza zone grigie.

Dalla disclosure alla governance

Rispettare l'articolo 50 non si esaurisce nel predisporre un avviso o un contrassegno: richiede un processo organizzativo verificabile nel tempo, non un adempimento isolato. In pratica, un'organizzazione dovrebbe:

- censire tutte le interfacce e le funzioni generative esistenti (chatbot, assistenti virtuali, strumenti che producono contenuti sintetici);
- definire quando e in che forma viene fornita l'informativa all'utente;
- verificare che tale informativa sia effettivamente accessibile;
- testare che i contrassegni sui contenuti generati persistano anche dopo condivisione, conversione di formato o pubblicazione su piattaforme terze;
- conservare evidenza delle soluzioni adottate, in modo da poterle dimostrare in caso di controllo.

Un'attenzione specifica va riservata alle tecnologie fornite da terzi quali soluzioni white-label, API, componenti integrati: l'organizzazione deve verificare che la ripartizione contrattuale delle attività rifletta il ruolo regolatorio effettivamente svolto (provider o deployer), perché l'etichetta usata nel contratto non è decisiva se la sostanza dei fatti è diversa.

Sul fronte della trasparenza dei contenuti generati dall'AI, la Commissione ha pubblicato linee guida, un documento di domande e risposte e un Codice di buone pratiche sulla trasparenza dei contenuti generati dall'AI , da non confondere con il Codice di buone pratiche per i modelli GPAI, dedicato invece a copyright, sicurezza e rischio sistemico dei modelli general-purpose. L'adesione al primo codice è volontaria: chi aderisce può dimostrare la conformità attraverso le misure previste dal codice stesso; chi non aderisce deve comunque dimostrare la conformità con mezzi alternativi adeguati, che resta a proprio carico individuare e documentare.

Le sanzioni per la violazione dell'articolo 50

La mancata conformità all'articolo 50 espone a sanzioni amministrative fino a **15 milioni di euro** o, per le imprese, fino al **3% del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore. Come per le altre sanzioni previste dall'AI Act, si applicano i massimali ridotti previsti per le **PMI, incluse le startup, e le piccole imprese a media capitalizzazione (SMC)**, un elemento che riguarda una parte significativa delle organizzazioni italiane ed europee soggette al Regolamento. Ogni sanzione deve comunque essere determinata caso per caso e restare effettiva, proporzionata e dissuasiva.

4. Dati particolari e bias: una base eccezionale, non una scorciatoia

Il nuovo **articolo 4-bis**, consente, in condizioni rigorose, il trattamento eccezionale di categorie particolari di dati personali per individuare e correggere bias. La disposizione si aggiunge al GDPR e alle altre regole europee applicabili: non costituisce un'autorizzazione generale a raccogliere dati sensibili.

Per i provider di sistemi ad alto rischio, il trattamento deve essere strettamente necessario rispetto agli obiettivi di cui **all'articolo 10, paragrafo 2, lettere f) e g)**, e solo se sono soddisfatte tutte le condizioni previste dall'**articolo 4-bis**. Tra le condizioni previste rientrano:

- l'impossibilità di conseguire efficacemente lo scopo mediante altri dati, inclusi dati sintetici o anonimizzati;
- limitazioni tecniche al riutilizzo, misure di sicurezza e tecniche di tutela della privacy allo stato dell'arte, inclusa la pseudonimizzazione;
- controlli stringenti sugli accessi e divieto di trasmissione, trasferimento o accesso da parte di altri soggetti;
- cancellazione dopo la correzione del bias o alla scadenza del periodo di conservazione, se anteriore;
- motivazione, nei registri delle attività di trattamento, della stretta necessità e dell'impossibilità di utilizzare dati alternativi.

La possibilità è estesa, alle condizioni indicate dalla norma, anche ai provider e deployer di altri sistemi e modelli, nonché ai deployer di sistemi ad alto rischio, quando il bias possa incidere sulla salute o sicurezza, sui diritti fondamentali o determinare discriminazioni vietate. Per tali soggetti la disposizione non crea, di per sé, un obbligo generale di svolgere questa specifica attività di bias detection e correction, come chiarisce espressamente l'art. 4-bis.

DECISIONE DI GOVERNANCE

Prima di utilizzare l'articolo 4-bis occorre un dossier di necessità: finalità, alternative scartate, categorie di dati, accessi, misure tecniche, tempi di cancellazione e responsabilità. L'eccezione deve essere dimostrabile, non soltanto dichiarata.

5. GPAI: obblighi già in vigore, enforcement rafforzato

Gli obblighi sostanziali del Capo V per i provider di modelli di AI per finalità generali sono applicabili dal 2 agosto 2025, con il regime transitorio previsto per i modelli immessi sul mercato in precedenza. Essi comprendono, tra l'altro, documentazione tecnica, informazioni per i provider a valle, una policy sul rispetto del diritto d'autore dell'Unione e una sintesi pubblica sufficientemente dettagliata dei contenuti utilizzati per l'addestramento. Ulteriori obblighi riguardano i modelli con rischio sistemico.

Dal 2 agosto 2026 diventa applicabile l'articolo 101. La Commissione può irrogare ai provider di modelli GPAI, per le violazioni intenzionali o colpose indicate dalla norma, sanzioni fino al 3% del fatturato mondiale totale annuo dell'esercizio precedente o a 15 milioni di euro, se superiore. Anche in questo caso si applicano, ove pertinenti, i massimali ridotti previsti per le PMI e le startup. I provider di modelli immessi sul mercato prima del 2 agosto 2025 dispongono fino al 2 agosto 2027 per adottare le misure necessarie.

L'uso di un modello di terzi non trasforma automaticamente un'organizzazione nel provider di quel modello. Può tuttavia renderla provider del sistema che lo integra oppure deployer. La qualificazione deve seguire le attività effettive, incluse modifiche, rebranding, integrazione e finalità dichiarate, non l'etichetta utilizzata nel contratto.

6. Gli obblighi che non hanno atteso il 2026

AI literacy: una responsabilità organizzativa

L'articolo 4 si applica dal 2 febbraio 2025. Provider e deployer devono adottare misure per sostenere lo sviluppo dell'alfabetizzazione in materia di AI del personale e delle altre persone che, per loro conto, operano o utilizzano sistemi di AI. Il contenuto deve tenere conto delle conoscenze tecniche, dell'esperienza, dell'istruzione, della formazione, del contesto d'uso e delle persone o gruppi sui quali i sistemi sono impiegati.

Dopo il Digital Omnibus, la norma chiarisce che non è richiesto garantire un livello specifico di alfabetizzazione per ciascun individuo. Non prescrive neppure un numero minimo di ore, una certificazione obbligatoria o un formato unico. Questa flessibilità non elimina l'obbligo: richiede una scelta proporzionata e documentabile.

- **Approccio coerente:** formazione differenziata per ruoli, responsabilità e casi d'uso.
- **Approccio debole:** un webinar generale uguale per tutti e scollegato dai sistemi realmente utilizzati.
- **Evidenza utile:** registro delle iniziative, destinatari, contenuti, aggiornamenti e collegamento ai rischi operativi.

Un programma credibile dovrebbe includere, secondo pertinenza, usi consentiti e vietati, limiti dei sistemi, output inesatti o discriminatori, gestione di dati personali e informazioni riservate, verifica umana, escalation e segnalazione degli incidenti.

Pratiche vietate: il controllo deve precedere l'adozione

Le pratiche originariamente vietate dall'articolo 5 sono applicabili dal 2 febbraio 2025. Ogni organizzazione dovrebbe quindi svolgere uno screening del caso d'uso prima dell'acquisto, dell'immissione sul mercato, della messa in servizio o dell'utilizzo del sistema.

Il Digital Omnibus introduce inoltre divieti relativi a sistemi che generano o manipolano materiale intimo realistico non consensuale riferibile a persone identificabili e materiale di abuso sessuale su minori. Questi nuovi divieti, con le relative condizioni e disposizioni di ambito, si applicano dal 2 dicembre 2026. Per i provider assumono rilievo anche l'uso improprio ragionevolmente prevedibile e riproducibile e l'adeguatezza delle misure tecniche e delle altre salvaguardie.

PRINCIPIO OPERATIVO

Un controllo ex post può essere tardivo: la verifica delle pratiche vietate deve essere incorporata nei processi di ideazione, procurement, approvazione e change management.

7. Usare il tempo aggiuntivo senza creare debito di compliance

Il rinvio del regime high-risk è utile solo se viene trasformato in un programma. Attendere la nuova scadenza significa accumulare sistemi, contratti e dipendenze difficili da ricostruire quando documentazione, controlli e responsabilità dovranno essere dimostrati.

Il regime transitorio dei sistemi già sul mercato

Per i sistemi ad alto rischio immessi sul mercato o messi in servizio prima della pertinente data di applicazione del Capo III, l'AI Act opera, in linea generale e fatto salvo l'articolo 5, se da quella data tali sistemi subiscono modifiche significative nel design. Il Digital Omnibus chiarisce che il regime si valuta rispetto al tipo e modello del sistema: se almeno un'unità è stata legittimamente immessa sul mercato o messa in servizio prima della data rilevante, ulteriori unità dello stesso tipo e modello possono beneficiare del regime finché il design resta invariato.

Una modifica significativa successiva fa scattare l'obbligo del provider di rispettare le disposizioni applicabili, inclusa la valutazione di conformità. Per i sistemi ad alto rischio destinati all'uso da parte di autorità pubbliche, provider e deployer devono in ogni caso adottare le misure necessarie entro il 2 agosto 2030.

Le evidenze da preservare

- data e prova della prima immissione sul mercato o messa in servizio;
- identificazione univoca di tipo, modello e versione;
- finalità prevista e design baseline;
- registro delle modifiche, con valutazione della loro significatività;
- responsabilità interne e informazioni ricevute dai fornitori.

Queste evidenze consentono di sostenere sia l'applicabilità del regime transitorio sia la valutazione delle modifiche intervenute nel tempo.

8. Il modello operativo: cinque capacità da costruire

L’adeguamento all’AI Act non può essere affrontato come una somma di adempimenti isolati. Richiede un modello di governance che colleghi sistemi, ruoli, responsabilità e controlli.

L’organizzazione deve innanzitutto conoscere quali sistemi e modelli di AI sviluppa, acquista o utilizza, per quali finalità e sotto la responsabilità di quali funzioni. Per ciascun caso d’uso deve poi chiarire il proprio ruolo regolatorio: provider, deployer o altro operatore della catena del valore.

Occorre inoltre definire chi può autorizzare, condizionare o sospendere l’utilizzo di un sistema. I controlli su trasparenza, dati, supervisione umana, sicurezza e pratiche vietate devono essere integrati nei processi di sviluppo, acquisto e utilizzo dell’AI.

Infine, inventari, valutazioni, test, contratti e registri delle modifiche devono consentire di ricostruire e dimostrare le decisioni adottate nel tempo.

MESSAGGIO CHIAVE

Non basta conoscere gli obblighi: occorre costruire un sistema organizzativo che li renda applicabili e dimostrabili.

9. Priorità per il management

L'adeguamento non può essere delegato integralmente alla funzione legale. Le decisioni riguardano prodotto, dati, tecnologia, persone, acquisti, comunicazione e controllo interno. Il management dovrebbe richiedere una vista unica del portafoglio e distinguere ciò che deve essere corretto subito da ciò che deve essere progettato per le scadenze future.

Le domande che il vertice dovrebbe porre

- Abbiamo un inventario affidabile o conosciamo soltanto i sistemi acquistati centralmente?
- Sappiamo in quali casi l'organizzazione cambia ruolo lungo la catena del valore?
- Le informative e i contrassegni sono presenti, accessibili, testati e coerenti tra canali?
- La formazione è collegata ai rischi reali dei ruoli o è un adempimento generico?
- Siamo in grado di ricostruire versioni, modifiche, approvazioni e basi decisionali?
- Le scadenze high-risk sono state tradotte in budget, responsabilità e milestone?

IL VERO RISCHIO

Non è soltanto interpretare male una data. È scoprire troppo tardi che nessuno possiede le informazioni, i poteri decisionali e le evidenze necessarie per governare il sistema.

10. Calendario essenziale

DATA	AMBITO	CHE COSA SIGNIFICA
2 febbraio 2025	AI literacy e pratiche vietate originarie	Articoli 4 e 5 applicabili, salvo i nuovi divieti introdotti nel 2026
2 agosto 2025	GPAI e altre disposizioni	Obblighi sostanziali per provider di modelli GPAI, con regole transitorie
27 luglio 2026	Digital Omnibus	Entrata in vigore del Reg. (UE) 2026/1744; Art 102-110 applicabili
2 agosto 2026	Trasparenza, art. 4-bis, enforcement GPAI	Articoli 50, 4-bis e 101 applicabili; fase rafforzata di vigilanza
2 dicembre 2026	Nuovi divieti e sistemi generativi preesistenti	Applicazione dei nuovi divieti; termine transitorio per l'art. 50(2)
2 agosto 2027	GPAI pre-2 agosto 2025	Termine per adottare le misure di conformità applicabili
2 dicembre 2027	High-risk Annex III	Capo III, Sez. 1-3 applicabili, salvo art. 6(5)
2 agosto 2028	High-risk Annex I	Capo III, Sez. 1-3 applicabili, salvo art. 6(5) e secondo le regole di ambito

2 agosto 2030	High-risk per autorità pubbliche	Termine specifico per le misure richieste a provider e deployer

Cosa fare ora

- Assegnare una responsabilità chiara per la conformità all'articolo 50.
- Integrare i requisiti di trasparenza nei framework di governance dell'IA già esistenti.
- Verificare i controlli tecnici per la marcatura e la rilevabilità dei contenuti generati dall'IA.
- Documentare, con un dossier di necessità, ogni eventuale ricorso all'articolo 4-bis.
- Preparare evidenze oggettive a supporto di futuri controlli regolatori e attività di vigilanza sul mercato.
- Aggiornare il programma di AI literacy sulla base dei sistemi effettivamente utilizzati, differenziando contenuti e modalità per ruoli, rischi e responsabilità.
- Documentare destinatari, contenuti, modalità, aggiornamenti e collegamento tra le iniziative di literacy e i rischi dei casi d'uso.

Le organizzazioni che agiscono ora si troveranno nella posizione migliore per dimostrare la conformità, ridurre il rischio di enforcement e costruire fiducia con clienti e regolatori mentre l'AI Act entra nella sua prossima fase attuativa.

Conclusioni: dalla scadenza alla capacità di governo

Il Digital Omnibus ridisegna il percorso di applicazione dell'AI Act, ma non riduce il bisogno di governo. Le organizzazioni devono oggi mantenere insieme tre prospettive: conformità immediata, costruzione progressiva del regime high-risk e controllo dell'evoluzione dei sistemi nel tempo.

Un programma efficace parte dall'inventario, ma non si esaurisce nella mappatura. Deve collegare ruoli regolatori, responsabilità aziendali, controlli tecnici, processi decisionali e produzione delle evidenze. In assenza di questo collegamento, il rischio è una compliance frammentata: corretta sulla carta, ma incapace di seguire l'effettiva vita dei sistemi.

LA SCELTA STRATEGICA

Usare il tempo aggiuntivo per costruire una capacità permanente di AI governance, invece di preparare un adeguamento concentrato nelle settimane che precedono la prossima scadenza.

Come Ainnova supporta le organizzazioni

Ainnova affianca imprese, istituzioni e organizzazioni pubbliche nella definizione di modelli di AI governance, nella classificazione dei sistemi, nella mappatura degli obblighi, nella costruzione delle roadmap di adeguamento e nei programmi di AI literacy. L'intervento integra prospettiva normativa, organizzativa e strategica, con l'obiettivo di trasformare la compliance in una capacità decisionale stabile.

Riferimenti e Fonti

Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio (Artificial Intelligence Act).
Regolamento (UE) 2026/1744 del Parlamento europeo e del Consiglio dell'8 luglio 2026 (Digital Omnibus on AI), GUUE del 24 luglio 2026.
Commissione europea, Guidelines on transparency obligations for providers and deployers of certain AI systems, aggiornamento 20 luglio 2026.
Commissione europea, Transparency obligations under Article 50 of the AI Act - Questions and answers, aggiornamento 24 luglio 2026.
Commissione europea, Commission starts enforcing AI Act rules and new transparency requirements on 2 August, 31 luglio 2026
Commissione europea, Draft Commission guidelines on the classification of high-risk AI systems, 19 maggio 2026

Il presente documento costituisce un'analisi orientativa e non vincolante, basata sul testo dell'AI Act, sul Digital Omnibus e sulle linee guida della Commissione europea disponibili alla data di pubblicazione. Il documento non costituisce parere legale e non sostituisce una valutazione specifica del caso concreto.