APPROFONDIMENTO NORMATIVO

AI Act: disposizioni applicabili dal 2 agosto 2026

Analisi del regolamento (UE) 2024/1689 come modificato dal regolamento (UE) 2026/1744

Digital Omnibus on AI

Aggiornamento al 27 luglio 2026

Sommario

Percorso di lettura

Sezione	Contenuto
Che cosa cambia, in sintesi	lettura immediata degli effetti del 2 agosto 2026; regole applicabili, rinvii, priorità e nota editoriale
Parte I - Guida applicativa	scadenze; verifiche per ruolo; checklist; errori interpretativi da evitare
Parte II - Approfondimento giuridico	fonti e calendario applicativo; articolo 50; alto rischio; modifiche del Digital Omnibus; disciplina italiana

Che cosa cambia, in sintesi

Dal 2 agosto 2026 l'AI Act entra in una nuova fase applicativa. La priorità immediata riguarda la trasparenza di determinati sistemi e contenuti, l'operatività delle sanzioni per i fornitori di modelli di IA per finalità generali e il rafforzamento degli strumenti di innovazione, governance e vigilanza. Il Digital Omnibus ha invece differito il nucleo della disciplina dei sistemi ad alto rischio.

Le tre cose da sapere

Dal 2 agosto 2026	Era già applicabile	È stato rinviato
• articolo 50 sulla trasparenza • articolo 101 e sanzioni GPAI • innovazione, prove, banca dati e vigilanza nei limiti applicabili	• pratiche vietate originarie • alfabetizzazione in materia di IA • obblighi dei fornitori di modelli GPAI • governance europea già operativa	• classificazione dell'alto rischio • requisiti degli articoli 8-15 • obblighi degli articoli 16-27 • FRIA e adempimenti collegati

Che cosa fare subito

Entro la data di applicazione occorre verificare i casi d'uso interessati dall'articolo 50, assicurare che contratti e interfacce consentano di rispettare gli obblighi di trasparenza, documentare il presidio editoriale dei testi di interesse pubblico e mantenere separati gli adempimenti dell'AI Act da quelli derivanti dal GDPR, dal diritto del lavoro e dalla disciplina nazionale.

Nota editoriale e articolo 50. La presente pubblicazione è posta sotto la responsabilità editoriale di iSimply s.r.l. Il testo finale è sottoposto, prima della diffusione, a revisione giuridica sostanziale e controllo editoriale umano. Strumenti di intelligenza artificiale sono stati impiegati come supporto alla ricerca, all'organizzazione e alla redazione; le affermazioni normative sono state verificate sulle fonti primarie indicate nel documento.

Parte I - Guida applicativa

Dal 2 agosto 2026 l'AI Act compie un nuovo passaggio applicativo. Per chi deve decidere o organizzarsi, il punto essenziale è questo: da quella data diventano operativi soprattutto gli obblighi di trasparenza, le sanzioni per i fornitori di modelli di IA per finalità generali e alcuni strumenti di governance, innovazione e vigilanza. Non diventa invece ancora applicabile la disciplina sostanziale dei sistemi di IA ad alto rischio, rinviata dal Digital Omnibus.

In 30 secondi: che cosa succede dal 2 agosto 2026

1. Trasparenza. Dal 2 agosto 2026 diventano applicabili gli obblighi dell'articolo 50. Nella pratica, ciò riguarda soprattutto chatbot e altri sistemi che interagiscono con persone fisiche, contenuti sintetici, deepfake e alcuni testi destinati a informare il pubblico.

2. Sanzioni per i fornitori di GPAI. Dal 2 agosto 2026 diventa applicabile l'articolo 101. Gli obblighi per i modelli di IA per finalità generali erano già applicabili dal 2 agosto 2025; da questa data è però operativo anche il relativo presidio sanzionatorio della Commissione europea.

3. Innovazione, vigilanza e governance. Dal 2 agosto 2026 si applicano anche disposizioni su spazi di sperimentazione, prove in condizioni reali, banca dati europea e vigilanza del mercato, nei limiti in cui non presuppongano la disciplina dell'alto rischio rinviata.

4. Alto rischio rinviato. Il Digital Omnibus ha rinviato la classificazione dei sistemi ad alto rischio, i requisiti degli articoli 8-15 e gli obblighi degli articoli 16-27. Le nuove date chiave sono il 2 dicembre 2027 per i sistemi dell'allegato III e il 2 agosto 2028 per i sistemi collegati all'allegato I.

Tre domande da porsi subito

Stiamo usando sistemi che interagiscono con persone? Se sì, la prima verifica riguarda l'informazione da rendere all'utente e, più in generale, la trasparenza dell'interazione.

Stiamo generando, pubblicando o diffondendo contenuti creati o manipolati dall'IA? Se sì, occorre verificare se si applicano obblighi di marcatura leggibile meccanicamente, etichettatura dei deepfake o trasparenza per i testi di interesse pubblico.

Siamo solo utilizzatori o abbiamo un ruolo più vicino a quello di fornitore? Quando il sistema viene personalizzato, integrato, rebrandizzato o modificato in modo rilevante, la distribuzione delle responsabilità deve essere analizzata con particolare attenzione.

Che cosa entra in applicazione e che cosa no

Entra in applicazione dal 2 agosto 2026. Gli obblighi di trasparenza dell'articolo 50; l'articolo 101 sulle sanzioni per i fornitori di GPAI; le disposizioni su innovazione, prove in condizioni reali, banca dati europea, monitoraggio e vigilanza, nei limiti compatibili con il rinvio dell'alto rischio.

Non entra ancora in applicazione dal 2 agosto 2026. La disciplina sostanziale dei sistemi di IA ad alto rischio: classificazione dei casi, requisiti degli articoli 8-15, obblighi degli articoli 16-27, FRIA e gli altri adempimenti specificamente collegati a quel blocco normativo.

Resta comunque necessario prepararsi. Il rinvio non giustifica inerzia: inventario dei sistemi, regole interne, contratti, controlli umani, governance dei dati e coordinamento con GDPR e disciplina nazionale devono essere impostati fin d'ora.

Schema visivo di sintesi

Infografica di sintesi del quadro applicabile dal 2 agosto 2026.

Che cosa fare subito in pratica

Se sviluppi o fornisci sistemi di IA, la prima verifica riguarda la trasparenza verso utenti e clienti, la marcatura dei contenuti sintetici quando richiesta e, se rilevante, il rapporto tra sistema e modello di IA per finalità generali.

Se utilizzi o integri sistemi di IA, devi verificare soprattutto se l'organizzazione pubblica deepfake o testi di interesse pubblico generati o manipolati dall'IA, se impiega sistemi di riconoscimento delle emozioni o di categorizzazione biometrica e se le informative sono rese in modo chiaro, tempestivo e accessibile.

Se operi nella pubblica amministrazione, restano centrali anche la legge n. 132/2025, il GDPR e le altre discipline settoriali. Il rinvio della disciplina dell'alto rischio non sospende gli obblighi nazionali e organizzativi già vigenti, né l'esigenza di tracciare gli usi dell'IA e di presidiare dati, responsabilità e controlli umani.

In ogni caso, il 2 agosto 2026 non è una data da gestire solo come scadenza formale. È il momento in cui occorre trasformare inventario dei sistemi, regole interne, contratti, informative e istruzioni operative in misure concretamente verificabili.

Scadenze essenziali

La tabella seguente riassume le principali date da monitorare e il relativo effetto operativo.

Data	Effetto principale	Azione immediata
27 luglio 2026	entrata in vigore del regolamento (UE) 2026/1744; applicabilità degli articoli da 102 a 110 e delle modifiche immediatamente operative	aggiornare il quadro normativo interno e le fonti utilizzate per la compliance
2 agosto 2026	obblighi di trasparenza dell'articolo 50; sanzioni GPAI dell'articolo 101; misure per innovazione, banca dati, vigilanza e ulteriori disposizioni non rinviate	attuare informative, marcature, procedure e conservazione delle evidenze
2 dicembre 2026	applicazione delle nuove pratiche vietate introdotte dal Digital Omnibus e termine transitorio per specifici sistemi generativi già immessi sul mercato	verificare i nuovi divieti e l'adeguamento dei sistemi generativi preesistenti
2 dicembre 2027	classificazione, requisiti e obblighi relativi ai sistemi ad alto rischio dell'allegato III	completare classificazione e piano di conformità per i sistemi dell'allegato III
2 agosto 2028	classificazione, requisiti e obblighi relativi ai sistemi ad alto rischio collegati ai prodotti dell'allegato I	completare il programma di conformità per i sistemi collegati ai prodotti dell'allegato I
2 agosto 2030	termine specifico per l'adeguamento dei sistemi ad alto rischio preesistenti destinati all'uso da parte delle autorità pubbliche	pianificare e documentare l'adeguamento dei sistemi pubblici preesistenti

Le sezioni che seguono trasformano il quadro normativo in verifiche pratiche, differenziate per ruolo, e in una checklist utilizzabile per assegnare responsabilità, raccogliere evidenze e documentare l'adeguamento.

Guida operativa per ruolo

Fornitori di sistemi di IA

Entro il 2 agosto 2026, il fornitore deve verificare almeno:

- se il sistema interagisce direttamente con persone fisiche e se l'informazione è effettivamente incorporata nella progettazione;
- se il sistema genera contenuti sintetici e se, quando richiesto, gli output sono marcati e rilevabili in formato leggibile meccanicamente;
- se opera il periodo transitorio fino al 2 dicembre 2026;
- se le eccezioni per editing standard o modifica non sostanziale sono documentabili;
- se la documentazione tecnica e contrattuale consente al deployer di mantenere la trasparenza nell'interfaccia finale;
- se il sistema è basato su un modello di IA per finalità generali e ricade nella competenza dell'Ufficio per l'IA.

Deployer

Il deployer deve verificare almeno:

- se utilizza sistemi di riconoscimento delle emozioni o categorizzazione biometrica;
- se pubblica deepfake o testi di interesse pubblico generati o manipolati dall'IA;
- se l'etichettatura è resa al momento corretto, in forma chiara, distinguibile e accessibile;
- se è presente una revisione umana sostanziale e una responsabilità editoriale identificata;
- se la personalizzazione, il rebranding o la modifica del sistema possono determinare l'assunzione del ruolo di fornitore;
- se permangono obblighi autonomi ai sensi del GDPR, della normativa del lavoro o di settore.

Fornitori di modelli di IA per finalità generali

Devono essere verificate:

- conformità agli articoli 53 e 55, secondo il caso;
- documentazione e informazioni per i fornitori a valle;
- politica sul rispetto del diritto d'autore;
- sintesi dei contenuti utilizzati per l'addestramento;
- obblighi per modelli con rischio sistemico;
- capacità di rispondere a richieste e controlli della Commissione;
- esposizione al regime sanzionatorio dell'articolo 101 dal 2 agosto 2026.

Pubbliche amministrazioni

Le amministrazioni dovrebbero disporre almeno di:

- inventario aggiornato dei sistemi di IA e dei relativi ruoli;
- classificazione preliminare dei casi d'uso, senza confondere la preparazione con l'applicabilità immediata degli obblighi ad alto rischio;
- regole interne su trasparenza, revisione umana, responsabilità e tracciabilità;
- presidi per evitare l'inserimento non autorizzato di dati personali, riservati o classificati nei sistemi generativi;
- clausole contrattuali su dati, marcatura, logging, audit, aggiornamenti, incidenti, portabilità e cooperazione;
- misure documentate di alfabetizzazione in materia di IA;
- raccordo tra responsabile per la transizione digitale, sicurezza, protezione dei dati, procurement, uffici legali e strutture utilizzatrici.

Checklist finale delle azioni prioritarie

Area	Verifica prioritaria	Evidenza raccomandata
Inventario	censire sistemi, modelli, fornitori, deployer e casi d'uso	registro dei sistemi di IA con proprietario interno e stato di conformità
Articolo 50, paragrafo 1	informazione nell'interazione diretta	schermate, specifiche di interfaccia, test e istruzioni
Articolo 50, paragrafo 2	marcatura leggibile meccanicamente	specifiche tecniche, test di rilevabilità, dichiarazione del fornitore
Articolo 50, paragrafo 3	informazione per emozioni e biometria	informativa contestuale, valutazione privacy, base giuridica e DPIA
Articolo 50, paragrafo 4	etichettatura di deepfake e testi di interesse pubblico	procedura editoriale, etichette ove dovute, nominativo del revisore, approvazione e responsabilità della pubblicazione
Accessibilità	informazioni conformi ai requisiti applicabili	test di accessibilità e verifica delle interfacce
Alfabetizzazione IA	misure proporzionate a ruoli e contesto	piano formativo, istruzioni, registri delle attività e verifiche
GPAI	conformità al capo V e preparazione all'articolo 101	fascicolo di conformità, responsabilità e flussi informativi
Sistemi ad alto rischio	programma di preparazione alle nuove scadenze	classificazione preliminare, roadmap 2027-2028 e piano di adeguamento
Contratti	obblighi di cooperazione, audit e aggiornamento	clausole, allegati tecnici, SLA e procedure di incident management

Area	Verifica prioritaria	Evidenza raccomandata
Privacy	coordinamento con GDPR e disciplina nazionale	registro trattamenti, DPIA, informative, accordi articolo 28 GDPR
PA	tracciabilità, supporto e responsabilità umana	regolamento interno, istruzioni operative, verbali e audit

Errori di lettura da evitare

Non sono giuridicamente corretti i seguenti assunti:

- «L'AI Act entra in vigore il 2 agosto 2026». È entrato in vigore il 1° agosto 2024;
- «Il Digital Omnibus ha rinviato tutto l'AI Act». Ha rinviato specificamente le sezioni 1, 2 e 3 del capo III;
- «Dal 2 agosto 2026 tutti i sistemi dell'allegato III devono applicare gli articoli da 8 a 27». Tali disposizioni sono rinviate al 2 dicembre 2027;
- «Il periodo transitorio fino al 2 dicembre 2026 riguarda tutti gli obblighi di trasparenza». Riguarda soltanto l'articolo 50, paragrafo 2, per sistemi immessi sul mercato prima del 2 agosto 2026;
- «La revisione umana esclude sempre l'obbligo di etichettatura». L'eccezione riguarda i testi di interesse pubblico e richiede anche una responsabilità editoriale identificata;
- «L'informazione prevista dall'articolo 50 sostituisce l'informativa privacy». I due obblighi hanno oggetto e funzione differenti;
- «Le linee guida AgID in bozza sono già vincolanti». Alla data del documento il relativo iter non risulta concluso;
- «Il rinvio degli obblighi ad alto rischio consente di sospendere GDPR, obblighi di sicurezza o normativa nazionale». Le discipline continuano ad applicarsi autonomamente.

Parte II - Approfondimento giuridico

Questa parte ricostruisce il fondamento normativo delle indicazioni operative, chiarendo il calendario applicativo, il contenuto delle disposizioni che diventano applicabili, gli effetti del rinvio dei sistemi ad alto rischio e il coordinamento con la disciplina italiana.

Come leggere questo approfondimento

Obiettivo dell'analisi

Il presente approfondimento ricostruisce il quadro normativo applicabile alla data del 2 agosto 2026, tenendo conto delle modifiche introdotte dal regolamento (UE) 2026/1744.

L'analisi persegue quattro obiettivi:

- individuare puntualmente le disposizioni che divengono applicabili dal 2 agosto 2026;
- chiarire quali disposizioni erano già applicabili e quali sono state rinviate;
- illustrare le modifiche apportate dal Digital Omnibus al testo originario dell'AI Act;
- fornire indicazioni operative differenziate per fornitori, deployer, fornitori di modelli di IA per finalità generali e pubbliche amministrazioni.

Fonti utilizzate e stato dei documenti

La ricostruzione è fondata prioritariamente sulle fonti normative ufficiali:

- regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, pubblicato nella GUUE L del 12 luglio 2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj;
- regolamento (UE) 2026/1744 del Parlamento europeo e del Consiglio, dell'8 luglio 2026, pubblicato nella GUUE L del 24 luglio 2026, ELI: http://data.europa.eu/eli/reg/2026/1744/oj;
- legge 23 settembre 2025, n. 132, nel testo vigente pubblicato su Normattiva e nella Gazzetta ufficiale della Repubblica italiana, ELI: https://www.normattiva.it/eli/id/2025/09/25/25G00143/CONSOLIDATED.

Sono inoltre considerati, con valore interpretativo e non legislativo, gli orientamenti della Commissione europea del 20 luglio 2026 sull'articolo 50 e il Codice di buone pratiche sulla trasparenza dei contenuti generati dall'IA. Tali documenti sono utilizzati esclusivamente per chiarire l'attuazione pratica degli obblighi e non per modificare il contenuto della fonte normativa.

I documenti AgID sull'adozione, lo sviluppo e il procurement di sistemi di IA nella pubblica amministrazione non sono utilizzati come fonte di obblighi vigenti. Alla data del presente documento, le linee guida sull'adozione risultano ancora nell'iter di adozione, mentre quelle su sviluppo e procurement sono pubblicate come bozze successive alla consultazione.

Come leggere le date dell'AI Act

L'entrata in vigore indica l'ingresso dell'atto nell'ordinamento. L'applicabilità individua il momento dal quale le singole disposizioni producono effetti obbligatori nei confronti dei destinatari.

L'AI Act è entrato in vigore il 1° agosto 2024. L'articolo 113 ha però previsto date differenziate di applicazione. Il Digital Omnibus, a sua volta, è entrato in vigore il 27 luglio 2026 e ha modificato direttamente l'articolo 113 e numerose altre disposizioni dell'AI Act.

Nel seguito, l'espressione «dal 2 agosto 2026» è pertanto riferita all'applicabilità e non all'entrata in vigore dell'AI Act.

Calendario applicativo dopo il Digital Omnibus

Calendario previsto dal testo originario

Nel testo originario, l'articolo 113 prevedeva:

- applicazione dei capi I e II dal 2 febbraio 2025;
- applicazione del capo III, sezione 4, del capo V, del capo VII, del capo XII e dell'articolo 78 dal 2 agosto 2025, con esclusione dell'articolo 101;
- applicazione generale dal 2 agosto 2026;
- applicazione dell'articolo 6, paragrafo 1, e dei corrispondenti obblighi dal 2 agosto 2027.

In base al calendario originario, la maggior parte della disciplina dei sistemi ad alto rischio dell'allegato III avrebbe dovuto essere applicabile dal 2 agosto 2026.

Calendario applicabile

Il regolamento (UE) 2026/1744 ha sostituito la lettera c) dell'articolo 113 e introdotto una nuova lettera d). Il calendario vigente è il seguente.

Data	Disposizioni e principali effetti
2 febbraio 2025	capi I e II, comprese definizioni, ambito di applicazione, alfabetizzazione in materia di IA e pratiche vietate originarie; restano escluse fino al 2 dicembre 2026 le nuove pratiche vietate introdotte dal Digital Omnibus
2 agosto 2025	capo III, sezione 4; capo V; capo VII; capo XII; articolo 78, con esclusione dell'articolo 101
27 luglio 2026	entrata in vigore del regolamento (UE) 2026/1744; applicazione espressa degli articoli da 102 a 110; operatività delle modifiche a disposizioni la cui data di applicazione era già trascorsa, tra cui la nuova definizione di componente di sicurezza e il nuovo articolo 4 bis, nei limiti del relativo ambito
2 agosto 2026	data generale residua di applicazione; articolo 50; articolo 101; capi VI, VIII, IX, X e XI e altre disposizioni non già applicabili o rinviate
2 dicembre 2026	nuove pratiche vietate dell'articolo 5, paragrafo 1, lettere b bis) e b ter), e paragrafi 1 bis e 1 ter; termine transitorio per l'adeguamento all'articolo 50, paragrafo 2, dei sistemi generativi immessi sul mercato prima del 2 agosto 2026
1 agosto 2027	termine per la pubblicazione degli orientamenti della Commissione sull'applicazione degli articoli 8, paragrafo 2, 9, paragrafo 10, e 17, paragrafo 3, secondo i principi di complementarità e proporzionalità per i sistemi dell'allegato I, sezione A
2 agosto 2027	termine entro cui deve essere operativo almeno uno spazio di sperimentazione normativa nazionale; termine per l'adozione degli atti delegati previsti dall'articolo 2, paragrafo 13, relativi alla limitazione di requisiti o obblighi quando la normativa settoriale offre una tutela equivalente o superiore
2 dicembre 2027	capo III, sezioni 1, 2 e 3, per i sistemi ad alto rischio ai sensi dell'articolo 6, paragrafo 2, e dell'allegato III
28 gennaio 2028	termine entro cui gli organismi già notificati ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, devono presentare domanda di designazione ai sensi della sezione 4 del capo III
2 agosto 2028	capo III, sezioni 1, 2 e 3, per i sistemi ad alto rischio ai sensi dell'articolo 6, paragrafo 1, e dell'allegato I
2 agosto 2030	termine specifico per l'adeguamento dei sistemi ad alto rischio preesistenti destinati a essere utilizzati dalle autorità pubbliche

Portata del rinvio per i sistemi ad alto rischio

Il rinvio riguarda esclusivamente le sezioni 1, 2 e 3 del capo III, ad eccezione dell'articolo 6, paragrafo 5.

Sono pertanto rinviati:

- gli articoli 6 e 7 sulla classificazione dei sistemi ad alto rischio, salvo l'articolo 6, paragrafo 5;
- gli articoli da 8 a 15 sui requisiti dei sistemi ad alto rischio;
- gli articoli da 16 a 27 sugli obblighi dei fornitori, dei rappresentanti autorizzati, degli importatori, dei distributori, dei deployer e sugli altri obblighi della catena del valore.

Il rinvio comprende, tra gli altri, il sistema di gestione del rischio, la governance dei dati, la documentazione tecnica, il logging, la trasparenza verso il deployer, la sorveglianza umana, l'accuratezza, la robustezza, la cybersicurezza, il sistema di gestione della qualità, gli obblighi specifici del deployer e la valutazione d'impatto sui diritti fondamentali dell'articolo 27.

Il rinvio modifica il momento in cui tali obblighi sono esigibili ai sensi dell'AI Act. Non sospende l'applicazione del GDPR, della normativa in materia di lavoro, non discriminazione, sicurezza dei prodotti, protezione dei consumatori, amministrazione digitale o delle disposizioni nazionali già vigenti.

Regole già applicabili prima del 2 agosto 2026

Principi generali, alfabetizzazione e pratiche vietate

Dal 2 febbraio 2025 sono applicabili:

- oggetto e ambito di applicazione del regolamento;
- definizioni;
- alfabetizzazione in materia di IA;
- pratiche di IA vietate previste dal testo originario.

Il Digital Omnibus ha modificato l'articolo 4 sull'alfabetizzazione in materia di IA. I fornitori e i deployer devono ora adottare misure volte a sostenere lo sviluppo dell'alfabetizzazione del personale e delle altre persone che utilizzano sistemi di IA per loro conto, tenendo conto delle conoscenze, dell'esperienza, dell'istruzione, della formazione, del contesto d'uso e delle persone sulle quali i sistemi sono utilizzati. La norma precisa che non è necessario garantire a ciascuna persona uno specifico livello predeterminato di alfabetizzazione.

La modifica non elimina l'obbligo. Ne conferma invece la natura proporzionata e contestuale. Una mera comunicazione generale, non collegata ai sistemi e alle attività effettivamente svolte, può risultare insufficiente a dimostrare l'adozione delle misure richieste.

Autorità di notifica e organismi di valutazione della conformità

Dal 2 agosto 2025 sono applicabili le disposizioni sulle autorità di notifica e sugli organismi notificati. Il Digital Omnibus ha introdotto procedure di domanda e valutazione unificate per gli organismi che operano anche nell'ambito della normativa settoriale di armonizzazione dell'Unione, al fine di ridurre duplicazioni.

Obblighi per i modelli di IA per finalità generali

Il capo V è applicabile dal 2 agosto 2025. Sono quindi già vigenti gli obblighi dei fornitori di modelli di IA per finalità generali, compresi gli obblighi di documentazione, informazione verso i fornitori a valle, politica sul diritto d'autore e pubblicazione di una sintesi sufficientemente dettagliata dei contenuti utilizzati per l'addestramento. Per i modelli con rischio sistemico trovano applicazione gli obblighi rafforzati previsti dall'articolo 55.

Dal 2 agosto 2026 diviene applicabile anche l'articolo 101, che completa il regime con il potere della Commissione di irrogare sanzioni pecuniarie.

Governance europea e disciplina sanzionatoria nazionale

Il capo VII e il capo XII, con esclusione dell'articolo 101, sono applicabili dal 2 agosto 2025. Sono quindi già operativi il quadro di governance e l'obbligo degli Stati membri di stabilire sanzioni e misure di esecuzione effettive, proporzionate e dissuasive.

Coordinamento con la normativa settoriale dell'Unione

Il Digital Omnibus ha anticipato espressamente al 27 luglio 2026 l'applicazione degli articoli da 102 a 110. Tali disposizioni coordinano l'AI Act con vari atti settoriali dell'Unione.

L'anticipazione evita un disallineamento con le modifiche apportate dal Digital Omnibus ai regolamenti relativi all'aviazione e alle macchine. La loro applicazione non equivale, tuttavia, all'anticipazione generale degli obblighi dei sistemi ad alto rischio, che rimangono assoggettati alle nuove date del 2027 e del 2028.

Regole che diventano applicabili dal 2 agosto 2026

Quali regole diventano operative dal 2 agosto 2026

L'articolo 113 continua a stabilire che l'AI Act si applica dal 2 agosto 2026, salvo le eccezioni espressamente indicate. La data opera quindi come regola generale residua.

Non è sufficiente individuare il capo o l'articolo formalmente applicabile. Occorre verificare se la disposizione presupponga la classificazione del sistema come ad alto rischio o l'applicazione di obblighi rinviati. In tali casi la norma può essere formalmente applicabile, ma non ancora concretamente esigibile rispetto a sistemi la cui disciplina sostanziale è stata differita.

Normazione, valutazione della conformità e registrazione

La sezione 5 del capo III comprende gli articoli da 40 a 49 e non è stata inserita nel rinvio. Dal 2 agosto 2026 risultano quindi applicabili le disposizioni relative a:

- norme armonizzate e prodotti della normazione;
- specifiche comuni;
- presunzioni di conformità;
- valutazione della conformità;
- certificati;
- registrazione;
- dichiarazione UE di conformità;
- marcatura CE.

La concreta esigibilità di molte di queste disposizioni presuppone però che un sistema sia assoggettato alla disciplina dei sistemi ad alto rischio. Poiché la classificazione e gli obblighi sostanziali delle sezioni 1, 2 e 3 sono rinviati, la sezione 5 svolge, sino alle nuove date, soprattutto una funzione di predisposizione istituzionale, tecnica e procedurale.

Non è quindi corretto concludere che ogni sistema potenzialmente incluso nell'allegato III debba essere marcato CE o registrato dal 2 agosto 2026. Tali obblighi divengono concretamente esigibili in coerenza con la data di applicazione del pertinente regime ad alto rischio.

Il Digital Omnibus ha inoltre:

- richiesto alla Commissione di promuovere prodotti della normazione che agevolino la conformità congiunta all'AI Act e alla normativa settoriale;
- introdotto una presunzione di conformità ai requisiti di cybersicurezza dell'articolo 15 quando ricorrono le condizioni previste dal regolamento (UE) 2024/2847, Cyber Resilience Act;
- semplificato le procedure di valutazione della conformità per i prodotti soggetti alla normativa dell'allegato I, sezione A;
- chiarito che la sola presenza di un componente di IA ad alto rischio non impone una valutazione da parte di terzi quando tale procedura non è richiesta dalla normativa settoriale applicabile.

Come informare persone e pubblico

L'articolo 50 costituisce il principale blocco di obblighi immediatamente rilevante per una vasta platea di organizzazioni.

Sistemi destinati a interagire direttamente con persone fisiche

Il fornitore deve garantire che il sistema sia progettato e sviluppato in modo che le persone siano informate di stare interagendo con un sistema di IA, salvo che ciò risulti evidente a una persona ragionevolmente informata, attenta e avveduta, considerate le circostanze e il contesto di utilizzo.

L'obbligo è posto dal paragrafo 1 sul fornitore. Quando il sistema è integrato o presentato al pubblico dal deployer, è tuttavia opportuno verificare che l'informazione predisposta dal fornitore non sia rimossa, oscurata o resa inefficace nell'interfaccia e nel concreto contesto d'uso.

L'eccezione per i sistemi autorizzati dalla legge a fini di accertamento, prevenzione, indagine o perseguimento dei reati è delimitata dal testo normativo e non può essere estesa a generiche finalità di sicurezza.

Marcatura dei contenuti sintetici

I fornitori di sistemi di IA, compresi i sistemi per finalità generali, che generano contenuti audio, immagini, video o testi sintetici devono garantire che gli output:

- siano marcati in formato leggibile meccanicamente;
- siano rilevabili come generati o manipolati artificialmente;
- utilizzino soluzioni efficaci, interoperabili, solide e affidabili nella misura tecnicamente possibile.

La valutazione deve tenere conto delle specificità e dei limiti dei contenuti, dei costi di attuazione, dello stato dell'arte e delle norme tecniche pertinenti.

L'obbligo non si applica quando il sistema svolge una funzione di assistenza per l'editing standard oppure non modifica in modo sostanziale i dati di input o la loro semantica. La portata dell'eccezione deve essere valutata in concreto e non consente di escludere automaticamente qualunque funzione di editing o rielaborazione.

Per i sistemi immessi sul mercato prima del 2 agosto 2026, il nuovo articolo 111, paragrafo 4, riconosce un periodo transitorio limitato: il fornitore deve adeguarsi all'articolo 50, paragrafo 2, entro il 2 dicembre 2026.

Il periodo transitorio:

- riguarda soltanto sistemi già immessi sul mercato prima del 2 agosto 2026;
- riguarda soltanto l'obbligo di marcatura e rilevabilità di cui al paragrafo 2;
- non rinvia gli obblighi dei paragrafi 1, 3, 4 e 5;
- non si estende indistintamente a ogni obbligo di trasparenza.

Riconoscimento delle emozioni e categorizzazione biometrica

Il deployer di un sistema di riconoscimento delle emozioni o di categorizzazione biometrica deve:

- informare le persone fisiche esposte al funzionamento del sistema;
- trattare i dati personali nel rispetto del GDPR, del regolamento (UE) 2018/1725 o della direttiva (UE) 2016/680, secondo il caso.

L'informazione non rende lecito un trattamento privo di base giuridica né consente un impiego vietato dall'articolo 5. In particolare, il riconoscimento delle emozioni nei luoghi di lavoro e negli istituti di istruzione rimane vietato, salvo gli impieghi ammessi per ragioni mediche o di sicurezza.

Deepfake

Il deployer di un sistema che genera o manipola immagini o contenuti audio o video costituenti un deepfake deve rendere noto che il contenuto è stato generato o manipolato artificialmente.

Per deepfake si intende un'immagine o un contenuto audio o video generato o manipolato dall'IA che assomiglia a persone, oggetti, luoghi, entità o eventi esistenti e che apparirebbe falsamente autentico o veritiero a una persona.

Per opere o programmi manifestamente artistici, creativi, satirici o fittizi, la comunicazione può essere resa in modo adeguato e non invasivo, senza ostacolare l'esposizione o il godimento dell'opera. La previsione non costituisce un'esenzione totale.

Testi destinati a informare il pubblico su questioni di interesse pubblico

Il deployer che genera o manipola mediante IA un testo pubblicato allo scopo di informare il pubblico su questioni di interesse pubblico deve rendere noto che il testo è stato generato o manipolato artificialmente.

L'obbligo non si applica quando ricorrono congiuntamente le seguenti condizioni:

- il contenuto è stato sottoposto a un processo di revisione umana o di controllo editoriale;
- una persona fisica o giuridica detiene la responsabilità editoriale della pubblicazione.

Secondo gli orientamenti della Commissione, la revisione umana richiede un esame deliberato della sostanza del contenuto da parte di una o più persone fisiche dotate di conoscenze pertinenti e giudizio professionale. Il controllo editoriale presuppone l'effettiva autorità di approvare, modificare o respingere il contenuto per ragioni sostanziali, comprese la verifica dei fatti e l'affidabilità delle fonti. Controlli meramente formali, ortografici o grammaticali non sono sufficienti. La responsabilità editoriale coincide con la responsabilità legale finale della pubblicazione.

Trasparenza e responsabilità editoriale di questo paper

Per oggetto e destinazione, questo paper è idoneo a rientrare tra i testi pubblicati allo scopo di informare il pubblico su questioni di interesse pubblico. L'eventuale utilizzo di sistemi di IA in funzione di supporto non comporta l'obbligo di etichettare il testo quando il contenuto finale è stato sottoposto a revisione umana sostanziale o a controllo editoriale e una persona fisica o giuridica assume la responsabilità editoriale della pubblicazione.

Per rendere verificabile questo presidio è opportuno conservare l'evidenza del revisore, delle fonti controllate, della data di approvazione e del soggetto che autorizza la diffusione. La nota editoriale inserita nel quadro essenziale ha funzione di trasparenza volontaria e documentale; non presuppone l'esistenza di un obbligo di etichettatura ai sensi dell'articolo 50, paragrafo 4.

Come deve essere resa l'informazione

Le informazioni previste dai paragrafi da 1 a 4 devono essere:

- chiare e distinguibili;
- fornite al più tardi al momento della prima interazione o esposizione;
- conformi ai requisiti di accessibilità applicabili.

L'articolo 50 non sostituisce gli obblighi informativi previsti dal GDPR, dalla normativa consumeristica, dal diritto del lavoro o da altre disposizioni nazionali ed europee.

Orientamenti e Codice di buone pratiche

La Commissione europea ha pubblicato il 20 luglio 2026 gli orientamenti sull'attuazione dell'articolo 50. Gli orientamenti costituiscono un riferimento interpretativo ufficiale, ma non modificano il testo del regolamento e non vincolano la Corte di giustizia.

Il Codice di buone pratiche sulla trasparenza dei contenuti generati dall'IA è uno strumento volontario. L'8 luglio 2026 la Commissione ha concluso che il Codice copre adeguatamente gli obblighi degli articoli 50, paragrafi 2, 4 e 5, e ne facilita l'attuazione; il 9 luglio 2026 il consiglio per l'IA ha adottato la propria valutazione di adeguatezza.

L'adesione al Codice non sostituisce l'obbligo normativo e non costituisce prova conclusiva della conformità. I soggetti non aderenti devono poter dimostrare con mezzi alternativi adeguati il rispetto dell'articolo 50.

Sanzioni per i fornitori di modelli di IA per finalità generali

Dal 2 agosto 2026 la Commissione può infliggere ai fornitori di modelli di IA per finalità generali sanzioni fino al 3 per cento del fatturato mondiale annuo totale dell'esercizio precedente o a 15 milioni di euro, se superiore, nei casi previsti dall'articolo 101.

L'articolo 101 completa il regime sostanziale del capo V, già applicabile dal 2 agosto 2025. La data del 2 agosto 2026 segna quindi il passaggio da un sistema di obblighi già vigenti a un quadro europeo dotato del relativo potere sanzionatorio specifico.

Sanzioni per la violazione degli obblighi di trasparenza

La violazione degli obblighi di trasparenza dell'articolo 50 rientra nell'articolo 99, paragrafo 4. La sanzione massima è pari a 15 milioni di euro o, per le imprese, al 3 per cento del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Per le PMI si applica il limite più basso tra l'importo assoluto e la percentuale. Il Digital Omnibus ha esteso un criterio analogo alle piccole imprese a media capitalizzazione.

L'articolo 99, paragrafo 8, consente agli Stati membri di stabilire in quale misura possano essere irrogate sanzioni amministrative pecuniarie alle autorità pubbliche e agli organismi pubblici. Tale facoltà non elimina gli altri poteri correttivi, di vigilanza e di limitazione dell'uso del sistema.

Sperimentazione e misure a sostegno dell'innovazione

Il capo VI diviene applicabile dal 2 agosto 2026. Il Digital Omnibus ha però modificato alcuni termini e ampliato le possibilità di sperimentazione.

Spazi di sperimentazione normativa

Il termine entro il quale ciascuno Stato membro deve rendere operativo almeno uno spazio di sperimentazione normativa nazionale è stato spostato dal 2 agosto 2026 al 2 agosto 2027.

Il quadro giuridico delle sandboxes diviene comunque applicabile dal 2 agosto 2026. Ne consegue che:

- le autorità possono istituire e gestire gli spazi secondo il capo VI;
- non si può presumere che dal 2 agosto 2026 ogni Stato disponga già di uno spazio nazionale operativo;
- la mancata disponibilità immediata dello spazio nazionale non rinvia gli altri obblighi applicabili.

Il Digital Omnibus consente inoltre all'Ufficio per l'IA di istituire uno spazio di sperimentazione a livello dell'Unione per i sistemi sottoposti alla propria competenza e rafforza il coinvolgimento delle autorità di protezione dei dati.

Prove in condizioni reali

Le modifiche ampliano le possibilità di prova in condizioni reali:

- l'articolo 60 è esteso ai sistemi disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A;
- il nuovo articolo 60 bis consente agli Stati membri di introdurre quadri di prova per i prodotti basati sull'IA disciplinati dall'allegato I, sezione B;
- restano ferme le tutele per salute, sicurezza, diritti fondamentali e protezione dei dati personali.

Banca dati europea dei sistemi di IA

Il capo VIII diviene applicabile dal 2 agosto 2026. La banca dati è destinata principalmente ai sistemi ad alto rischio dell'allegato III e ai sistemi per i quali il fornitore conclude che non ricorra la classificazione ad alto rischio ai sensi dell'articolo 6, paragrafo 3.

Poiché la classificazione e gli obblighi di registrazione collegati sono rinviati al 2 dicembre 2027, l'applicabilità del capo VIII non comporta, dal 2 agosto 2026, un obbligo generalizzato e autonomo di registrazione per tutti i sistemi potenzialmente compresi nell'allegato III.

La banca dati e le relative infrastrutture possono essere predisposte e rese operative, ma l'obbligo concreto di inserimento deve essere coordinato con le date applicabili alla classificazione e agli obblighi del singolo sistema.

Monitoraggio, reclami e vigilanza del mercato

Il capo IX diviene applicabile dal 2 agosto 2026, con l'eccezione dell'articolo 78, già applicabile dal 2 agosto 2025.

Il capo comprende disposizioni eterogenee:

- monitoraggio successivo all'immissione sul mercato;
- segnalazione degli incidenti gravi;
- vigilanza del mercato;
- poteri delle autorità;
- accesso alla documentazione;
- sistemi che presentano un rischio;
- diritto di presentare reclamo;
- diritto alla spiegazione dei processi decisionali individuali in determinati casi.

Le disposizioni strettamente riferite ai sistemi ad alto rischio devono essere lette in coordinamento con il rinvio delle sezioni 1, 2 e 3 del capo III. Non possono essere utilizzate per reintrodurre indirettamente, dal 2 agosto 2026, obblighi sostanziali che il legislatore europeo ha espressamente differito.

Rimangono invece operative le componenti generali del sistema di vigilanza e i poteri attribuiti alle autorità per le disposizioni già applicabili, in particolare per articolo 50, modelli di IA per finalità generali e pratiche vietate.

Poteri dell'Ufficio per l'IA

Il Digital Omnibus ha riscritto e ampliato l'articolo 75 e ha introdotto gli articoli da 75 bis a 75 quinquies.

L'Ufficio per l'IA acquisisce competenza esclusiva per la vigilanza e l'esecuzione in relazione, tra gli altri, a:

- sistemi basati su modelli di IA per finalità generali quando il modello e il sistema sono sviluppati dallo stesso fornitore o da soggetti appartenenti alla stessa impresa, salvo le eccezioni previste;
- sistemi che costituiscono o sono integrati in piattaforme online di dimensioni molto grandi o motori di ricerca online di dimensioni molto grandi designati ai sensi del Digital Services Act.

Sono disciplinati poteri di indagine, richiesta di informazioni, accesso e ispezione, imposizione di misure correttive, accettazione di impegni, sanzioni, penalità di mora e garanzie procedurali.

Codici di condotta, orientamenti e poteri della Commissione

Dal 2 agosto 2026 divengono applicabili:

- il capo X sui codici di condotta e sugli orientamenti;
- il capo XI sulla delega di potere e sulla procedura di comitato.

Il Digital Omnibus estende l'attenzione alle piccole imprese a media capitalizzazione e aggiorna i poteri delegati della Commissione, compresi quelli relativi alla limitazione di obblighi duplicativi per sistemi soggetti a normativa settoriale equivalente e alla modifica dell'elenco dei codici per gli organismi notificati.

Gli obblighi per i sistemi ad alto rischio che non si applicano ancora

Classificazione dei sistemi ad alto rischio

Le regole di classificazione delle sezioni 1 del capo III sono rinviate, salvo l'articolo 6, paragrafo 5.

Per i sistemi dell'allegato III, la classificazione e i relativi effetti divengono applicabili il 2 dicembre 2027. Per i sistemi collegati ai prodotti dell'allegato I, la data è il 2 agosto 2028.

L'articolo 6, paragrafo 5, è escluso dal rinvio. La disposizione richiede alla Commissione orientamenti sull'attuazione dell'articolo 6, corredati da esempi pratici di sistemi ad alto rischio e non ad alto rischio. Alla data del 27 luglio 2026 sono disponibili orientamenti in bozza, pubblicati il 19 maggio 2026 e sottoposti a consultazione fino al 23 luglio 2026; la versione definitiva non risulta ancora adottata.

Requisiti dei sistemi ad alto rischio

Non diventano applicabili il 2 agosto 2026 gli articoli da 8 a 15, relativi a:

- conformità ai requisiti;
- gestione del rischio;
- dati e governance dei dati;
- documentazione tecnica;
- registrazione automatica degli eventi;
- trasparenza e informazioni al deployer;
- sorveglianza umana;
- accuratezza, robustezza e cybersicurezza.

Obblighi di fornitori, deployer e altri operatori

Non diventano applicabili il 2 agosto 2026 gli articoli da 16 a 27, relativi a:

- obblighi del fornitore;
- sistema di gestione della qualità;
- conservazione della documentazione;
- log generati automaticamente;
- azioni correttive e cooperazione;
- rappresentante autorizzato;
- importatore;
- distributore;
- responsabilità lungo la catena del valore;
- obblighi del deployer;
- valutazione d'impatto sui diritti fondamentali.

Il differimento non impedisce l'applicazione di obblighi analoghi o concorrenti previsti da altre fonti. Una DPIA può essere obbligatoria ai sensi del GDPR anche quando l'articolo 27 dell'AI Act non è ancora applicabile. Analogamente, controlli umani, logging, misure di sicurezza e governance dei dati possono essere necessari ai sensi del GDPR, della NIS2, della normativa settoriale o di obblighi contrattuali.

Le altre modifiche introdotte dal Digital Omnibus

Nuova definizione di componente di sicurezza

Il Digital Omnibus ha circoscritto la definizione di «componente di sicurezza». Un componente svolge una funzione di sicurezza quando la sua finalità prevista consiste nel prevenire o attenuare rischi per la salute e la sicurezza delle persone o dei beni, oppure quando il suo guasto o malfunzionamento mette in pericolo tali interessi.

Non sono considerati componenti di sicurezza i sistemi destinati esclusivamente a:

- assistenza agli utenti;
- ottimizzazione delle prestazioni;
- efficienza dei servizi;
- automazione;
- praticità;
- controlli di qualità non connessi alla sicurezza.

La sola integrazione dell'IA in un prodotto regolamentato non determina automaticamente la classificazione ad alto rischio.

Quando producono effetti le nuove regole

La nuova definizione di componente di sicurezza è contenuta nell'articolo 3 e, quindi, nel capo I. È applicabile dal 27 luglio 2026 e può essere utilizzata sin d'ora nella ricognizione dei prodotti, nella progettazione e nella qualificazione preliminare dei componenti.

I nuovi paragrafi 1 bis, 1 ter e 1 quater dell'articolo 6 sono invece collocati nella sezione 1 del capo III. Per i sistemi collegati ai prodotti dell'allegato I seguono il rinvio al 2 agosto 2028. La definizione è dunque già operativa, mentre gli effetti classificatori e gli obblighi del capo III diverranno esigibili secondo il calendario differito.

Trattamento di categorie particolari di dati per il controllo delle distorsioni

Il nuovo articolo 4 bis, inserito nel capo I e applicabile dal 27 luglio 2026, disciplina il trattamento eccezionale di categorie particolari di dati personali per rilevare e correggere distorsioni.

Per i fornitori di sistemi ad alto rischio, il trattamento è consentito nella misura strettamente necessaria per adempiere alle finalità dell'articolo 10, paragrafo 2, lettere f) e g).

La possibilità è estesa, senza introdurre un autonomo obbligo di rilevamento, anche:

- ai fornitori e deployer di altri sistemi e modelli di IA;
- ai deployer di sistemi ad alto rischio;
- quando le distorsioni possono incidere sulla salute, sulla sicurezza, sui diritti fondamentali o determinare discriminazioni vietate.

Devono ricorrere tutte le garanzie previste, tra cui:

- impossibilità di ottenere efficacemente il risultato mediante altri dati, compresi dati sintetici o anonimizzati;
- limitazioni tecniche al riutilizzo;
- misure avanzate di sicurezza e tutela della vita privata;
- pseudonimizzazione;
- controlli e documentazione rigorosa degli accessi;
- divieto di trasmissione, trasferimento o accesso da parte di terzi;
- cancellazione al raggiungimento della finalità o alla scadenza della conservazione;
- motivazione nel registro delle attività di trattamento.

La disposizione costituisce una base specifica nel quadro dell'articolo 9, paragrafo 2, lettera g), GDPR, ma non esclude gli altri obblighi del diritto europeo sulla protezione dei dati. Rimangono necessari, secondo il caso, la definizione del ruolo, la base giuridica per i dati comuni, la minimizzazione, la DPIA, le misure di sicurezza e il rispetto dei diritti degli interessati.

La sua applicabilità immediata consente agli operatori interessati, quando ricorrono tutti i presupposti della disposizione, di avviare già nella fase preparatoria attività di rilevamento e correzione delle distorsioni. La norma non introduce tuttavia un obbligo generalizzato di trattare categorie particolari di dati e non sostituisce la valutazione complessiva richiesta dal GDPR.

Nuove pratiche vietate

Il Digital Omnibus introduce nuove pratiche vietate relative a:

- sistemi che generano o manipolano materiale intimo realistico non consensuale riferibile a una persona riconoscibile;
- sistemi che generano o manipolano materiale o spettacoli di abuso sessuale su minori ai sensi della direttiva 2011/93/UE.

Le nuove disposizioni precisano separatamente i presupposti del divieto per fornitori e deployer e le condizioni relative alle misure tecniche di sicurezza.

Tali divieti si applicano dal 2 dicembre 2026, non dal 2 agosto 2026.

Semplificazioni per PMI e piccole imprese a media capitalizzazione

Il Digital Omnibus introduce la definizione di piccola impresa a media capitalizzazione e amplia a tale categoria alcune misure di proporzionalità e sostegno.

Le modifiche riguardano, tra l'altro:

- documentazione tecnica semplificata;
- proporzionalità del sistema di gestione della qualità;
- orientamenti e assistenza delle autorità;
- accesso prioritario agli spazi di sperimentazione;
- criteri sanzionatori proporzionati.

La semplificazione non riduce il livello di protezione richiesto e non costituisce un'esenzione sostanziale dagli obblighi applicabili.

Catena del valore e cooperazione tra operatori

Le modifiche all'articolo 25 rafforzano gli obblighi di cooperazione tra il fornitore originario, il soggetto che assume successivamente il ruolo di fornitore e i terzi che forniscono sistemi, modelli, strumenti, servizi, componenti o processi integrati in sistemi ad alto rischio.

Sono richiesti, nei casi previsti:

- documentazione tecnica sufficiente;
- comunicazione delle limitazioni note e delle modalità di guasto;
- accesso tecnico mirato per sperimentazione e convalida;
- accordi scritti sulle informazioni, sulle capacità, sull'accesso tecnico e sull'assistenza necessaria.

La disciplina resta assoggettata alle date di applicazione del capo III, sezione 3, ma deve essere considerata già nella contrattualistica e nel procurement, poiché incide sulla futura capacità di dimostrare la conformità.

Coordinamento tra valutazione d'impatto sui diritti fondamentali e DPIA

Il nuovo articolo 27, paragrafo 4, chiarisce che il deployer può richiamare o incorporare nella valutazione d'impatto sui diritti fondamentali le parti pertinenti di una DPIA già svolta ai sensi del GDPR o della direttiva (UE) 2016/680.

La modifica riduce duplicazioni documentali, ma non identifica le due valutazioni. Ambito, presupposti e oggetto rimangono distinti. L'integrazione è possibile soltanto per gli elementi effettivamente coincidenti.

Regime transitorio dei sistemi preesistenti

L'articolo 111, paragrafo 2, come modificato, stabilisce che i sistemi ad alto rischio immessi sul mercato o messi in servizio prima della pertinente data di applicazione del capo III sono soggetti ai nuovi obblighi soltanto se, a decorrere da quella data, sono sottoposti a modifiche significative della progettazione.

Il considerando 39 del Digital Omnibus chiarisce che il regime transitorio riguarda il tipo e il modello già legittimamente immesso sul mercato o messo in servizio. Ulteriori unità dello stesso tipo e modello possono beneficiare del regime transitorio finché la progettazione rimane invariata.

Per i sistemi ad alto rischio destinati all'uso da parte delle autorità pubbliche è previsto comunque l'adeguamento entro il 2 agosto 2030.

Il regime transitorio non esclude l'applicazione delle pratiche vietate, dell'articolo 50, del GDPR e delle altre normative applicabili.

Coordinamento con la disciplina italiana

Legge 23 settembre 2025, n. 132

La legge n. 132/2025 è in vigore dal 10 ottobre 2025. L'articolo 1, comma 2, stabilisce che le disposizioni nazionali devono essere interpretate e applicate conformemente all'AI Act.

L'articolo 3, comma 5, precisa che la legge non produce nuovi obblighi rispetto a quelli previsti dall'AI Act per i sistemi e i modelli di IA. La legge contiene tuttavia principi, disposizioni settoriali, regole organizzative e attribuzioni di competenza già applicabili nell'ordinamento nazionale.

Sono particolarmente rilevanti:

- articolo 11, sull'uso dell'IA in materia di lavoro;
- articolo 13, sulle professioni intellettuali;
- articolo 14, sull'uso dell'IA nella pubblica amministrazione;
- articolo 20, sulle autorità nazionali per l'intelligenza artificiale.

Il rinvio europeo delle sezioni 1, 2 e 3 del capo III non sospende tali disposizioni nazionali.

Pubblica amministrazione

L'articolo 14 della legge n. 132/2025 stabilisce che le pubbliche amministrazioni utilizzano l'IA per incrementare l'efficienza, ridurre i tempi e migliorare i servizi, assicurando:

- conoscibilità del funzionamento;
- tracciabilità dell'utilizzo;
- funzione strumentale e di supporto rispetto all'attività provvedimentale;
- permanenza della responsabilità decisionale in capo alla persona;
- misure tecniche, organizzative e formative per un utilizzo responsabile.

Tali obblighi sono già vigenti e devono essere coordinati con l'articolo 50 dal 2 agosto 2026.

Lavoro e professioni intellettuali

In ambito lavorativo, la legge n. 132/2025 impone sicurezza, affidabilità, trasparenza, rispetto della dignità e della riservatezza, oltre agli obblighi informativi previsti dalla disciplina nazionale sul rapporto di lavoro.

Per le professioni intellettuali, l'IA deve avere funzione strumentale e di supporto e deve rimanere prevalente il lavoro intellettuale del professionista. L'utilizzo dei sistemi deve essere comunicato al destinatario della prestazione con linguaggio chiaro, semplice ed esaustivo.

Linee guida AgID

Alla data del 27 luglio 2026:

- le linee guida AgID per l'adozione dell'IA nella pubblica amministrazione risultano ancora nell'iter di adozione;
- le linee guida per lo sviluppo e il procurement sono state sottoposte a consultazione pubblica nel 2026 e risultano ancora pubblicate come bozze.

Le bozze possono costituire un utile parametro tecnico e organizzativo, ma non devono essere presentate come fonte già vincolante. I regolamenti e i capitolati delle amministrazioni dovrebbero essere strutturati in modo da poter recepire la versione definitiva senza alterare l'impianto generale di governance.

Conclusioni

Il quadro applicabile dal 2 agosto 2026 è il risultato della combinazione tra la regola generale dell'articolo 113 e le eccezioni modificate dal regolamento (UE) 2026/1744.

Il Digital Omnibus non ha svuotato la scadenza del 2 agosto. Ha rinviato il blocco più oneroso della disciplina dei sistemi ad alto rischio, ma ha lasciato applicabili gli obblighi di trasparenza, il regime

sanzionatorio dei fornitori di modelli di IA per finalità generali, le misure di innovazione, la vigilanza e le ulteriori disposizioni non espressamente differite.

La priorità immediata per organizzazioni pubbliche e private è l'articolo 50. Gli operatori devono distinguere tra obblighi del fornitore e obblighi del deployer, verificare il limitato regime transitorio e mantenere separate la trasparenza AI Act, la trasparenza privacy e la responsabilità editoriale.

Parallelamente è necessario proseguire la preparazione per i sistemi ad alto rischio. Il rinvio al 2027 e al 2028 riduce l'urgenza formale, ma non elimina la necessità di inventariare i casi d'uso, assicurare la disponibilità delle informazioni contrattuali, definire responsabilità, pianificare la governance dei dati e prevenire il lock-in. Un'attesa passiva renderebbe difficile dimostrare la conformità quando le nuove scadenze diverranno operative.

Allegato A - Quadro sinottico delle modifiche introdotte dal Digital Omnibus

Disposizione modificata	Contenuto essenziale della modifica
Articolo 1, paragrafo 2, lettera g)	estensione delle misure a sostegno dell'innovazione alle piccole imprese a media capitalizzazione
Articolo 2, paragrafi 2, 7 e 13	delimitazione del regime per i prodotti dell'allegato I, sezione B; conferma della piena applicabilità della normativa privacy; possibilità di limitare duplicazioni quando la normativa settoriale offre tutela equivalente, con atti delegati da adottare entro il 2 agosto 2027
Articolo 3, punto 14)	nuova definizione di componente di sicurezza, applicabile dal 27 luglio 2026; la definizione può essere utilizzata immediatamente per la ricognizione e la progettazione, ferma la diversa data degli effetti classificatori del capo III
Articolo 3, punti 14 bis) e 14 ter)	introduzione delle definizioni di PMI e piccola impresa a media capitalizzazione, applicabili dal 27 luglio 2026
Articolo 4	riformulazione proporzionata dell'obbligo di alfabetizzazione in materia di IA
Nuovo articolo 4 bis	trattamento eccezionale di categorie particolari di dati per il rilevamento e la correzione delle distorsioni, alle condizioni rigorose previste dalla disposizione; applicabile dal 27 luglio 2026
Articolo 5	introduzione dei divieti relativi a materiale intimo non consensuale e materiale di abuso sessuale su minori, applicabili dal 2 dicembre 2026
Articolo 6, paragrafi 1 bis, 1 ter e 1 quater	chiarimenti sui sistemi che costituiscono componenti di sicurezza, sui malfunzionamenti rilevanti e sui controlli non riferiti a salute e sicurezza; per i sistemi dell'articolo 6, paragrafo 1, e dell'allegato I, applicabili dal 2 agosto 2028
Articolo 10	coordinamento della governance dei dati con il nuovo articolo 4 bis
Articolo 11	documentazione tecnica semplificata per PMI e piccole imprese a media capitalizzazione
Articolo 17	proporzionalità del sistema di gestione della qualità rispetto alle dimensioni dell'organizzazione
Articolo 25	cooperazione del fornitore originario e accordi scritti lungo la catena del valore
Articolo 27	possibilità di richiamare o incorporare parti pertinenti della DPIA nella valutazione d'impatto sui diritti fondamentali
Articoli 28-30 e nuovo allegato XIV	procedure unificate per designazione e notifica degli organismi di valutazione della conformità; gli organismi già notificati ai sensi dell'allegato I, sezione A, devono presentare domanda di designazione entro il 28 gennaio 2028
Articolo 40	normazione per la conformità congiunta all'AI Act e alla normativa settoriale
Articolo 42	coordinamento della presunzione di conformità in materia di cybersicurezza con il Cyber Resilience Act
Articolo 43	semplificazione e integrazione delle procedure di valutazione della conformità
Articolo 50, paragrafo 7	nuovo sistema di valutazione dei codici di buone pratiche sulla trasparenza
Articolo 56, paragrafo 6	monitoraggio e valutazione dei codici di buone pratiche GPAI senza approvazione mediante atto di esecuzione

Disposizione modificata	Contenuto essenziale della modifica
Articoli 57 e 58	termine nazionale sandbox al 2 agosto 2027; sandbox dell'Ufficio per l'IA; governance e coinvolgimento delle autorità privacy
Articolo 60	estensione delle prove in condizioni reali ai sistemi dell'allegato I, sezione A
Nuovo articolo 60 bis	quadri nazionali per prove in condizioni reali dei prodotti dell'allegato I, sezione B
Articolo 63	sistema di gestione della qualità semplificato per determinate PMI
Articolo 64	risorse adeguate per l'Ufficio per l'IA
Articolo 69	revisione delle tariffe relative all'assistenza degli esperti
Articolo 70	orientamenti e consulenza delle autorità, con attenzione a PMI e piccole imprese a media capitalizzazione
Articolo 72	orientamenti e modello per il piano di monitoraggio successivo all'immissione sul mercato entro il 2 settembre 2027
Articolo 75	competenza esclusiva dell'Ufficio per l'IA su specifici sistemi e coordinamento con le autorità nazionali
Nuovi articoli 75 bis-75 quinquies	poteri di indagine ed esecuzione, impegni, sanzioni, penalità di mora e garanzie procedurali
Articolo 76	coordinamento delle prove con il nuovo articolo 60 bis
Articolo 77	accesso delle autorità che tutelano i diritti fondamentali e cooperazione con la vigilanza del mercato
Articolo 95	attenzione a PMI, start-up e piccole imprese a media capitalizzazione nei codici di condotta
Articolo 96	aggiornamento degli orientamenti della Commissione e riduzione delle duplicazioni con la normativa settoriale; orientamenti su complementarità e proporzionalità da pubblicare entro il 1° agosto 2027
Articolo 97	aggiornamento delle deleghe conferite alla Commissione
Articolo 99	sanzioni applicabili a qualsiasi violazione; inserimento dell'articolo 25; proporzionalità per piccole imprese a media capitalizzazione
Articolo 111	regime transitorio per sistemi ad alto rischio preesistenti; adeguamento delle PA entro il 2030; periodo transitorio per articolo 50, paragrafo 2
Articolo 113	nuove date 2027 e 2028; nuove pratiche vietate dal 2 dicembre 2026; articoli 102-110 dal 27 luglio 2026
Allegato I	spostamento della disciplina delle macchine dalla sezione A alla sezione B
Allegato VIII	semplificazione delle informazioni da inserire nella banca dati europea
Regolamento (UE) 2018/1139	coordinamento dei requisiti AI Act con la normativa dell'aviazione civile
Regolamento (UE) 2023/1230	integrazione dei requisiti AI Act nella disciplina delle macchine e relativo coordinamento temporale

Allegato B - Fonti normative e documenti ufficiali

1. Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, GUUE L, 2024/1689, 12 luglio 2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj.
2. Regolamento (UE) 2026/1744 del Parlamento europeo e del Consiglio, dell'8 luglio 2026, GUUE L, 2026/1744, 24 luglio 2026, ELI: http://data.europa.eu/eli/reg/2026/1744/oj.

3. Legge 23 settembre 2025, n. 132, «Disposizioni e deleghe al Governo in materia di intelligenza artificiale», GU Serie Generale n. 223 del 25 settembre 2025, testo vigente su Normattiva: https://www.normattiva.it/eli/id/2025/09/25/25G00143/CONSOLIDATED.
4. Commissione europea, «Guidelines on the implementation of the transparency obligations for certain AI systems under Article 50 of the AI Act», 20 luglio 2026: https://digital-strategy.ec.europa.eu/en/library/guidelines-transparency-obligations-providers-and-deployers-ai-systems.
5. Commissione europea, «Code of Practice on Transparency of AI-Generated Content», versione finale 10 giugno 2026: https://digital-strategy.ec.europa.eu/en/policies/code-practice-ai-generated-content.
6. Commissione europea, «Commission Opinion on the assessment of the Code of Practice on Transparency of AI-generated content», adottata l'8 luglio 2026 e pubblicata il 9 luglio 2026: https://digital-strategy.ec.europa.eu/en/library/commission-opinion-assessment-code-practice-transparency-ai-generated-content.
7. European Artificial Intelligence Board, «AI Board Adequacy Assessment Code of Practice Transparency of AI-Generated Content», 9 luglio 2026: https://digital-strategy.ec.europa.eu/en/policies/ai-board.
8. Commissione europea, «Transparency obligations under Article 50 of the AI Act - Questions and answers», aggiornamento 24 luglio 2026: https://digital-strategy.ec.europa.eu/en/faqs/transparency-obligations-under-article-50-ai-act.
9. Commissione europea, «Draft Commission guidelines on the classification of high-risk AI systems», 19 maggio 2026, consultazione chiusa il 23 luglio 2026: https://digital-strategy.ec.europa.eu/en/library/draft-commission-guidelines-classification-high-risk-ai-systems.
10. AgID, pagina istituzionale «Intelligenza artificiale», stato delle linee guida alla data del documento: https://www.agid.gov.it/it/ambiti-intervento/intelligenza-artificiale.

Azioni consigliate per le organizzazioni

Le azioni seguenti non sostituiscono la valutazione del singolo sistema e del relativo ruolo giuridico. Costituiscono una sequenza operativa per rendere l'adeguamento dimostrabile, coordinato e proporzionato.

Priorità	Azione consigliata	Evidenza attesa
1	Censire sistemi, modelli, fornitori, deployer e casi d'uso, attribuendo un responsabile interno.	Registro dei sistemi di IA aggiornato e approvato.
2	Verificare i casi ricadenti nell'articolo 50 e distinguere gli obblighi del fornitore da quelli del deployer.	Matrice di applicabilità, schermate, etichette, specifiche e test.
3	Formalizzare revisione umana, controllo editoriale e responsabilità per testi di interesse pubblico.	Procedura editoriale, nominativi dei revisori, approvazione alla pubblicazione e tracciabilità delle fonti.
4	Aggiornare contratti e capitolati su marcatura, accessibilità, audit, logging, dati, incidenti e cooperazione.	Clausole contrattuali e allegati tecnici coerenti con i ruoli effettivi.
5	Documentare misure di alfabetizzazione in materia di IA proporzionate a ruoli, sistemi e contesto.	Piano formativo, istruzioni operative, registri e verifiche di efficacia.
6	Preparare il percorso per i sistemi potenzialmente ad alto rischio senza anticipare obblighi non ancora applicabili.	Classificazione preliminare, roadmap 2027-2028, gap analysis e piano di adeguamento.
7	Istituire un presidio di monitoraggio normativo e tecnico sulle fonti UE, nazionali e AgID.	Calendario di riesame, responsabilità assegnate e registro degli aggiornamenti.

Come rendere l'adeguamento verificabile

La conformità non si esaurisce nella presenza di una policy o di un’informativa. Deve poter essere ricostruita attraverso ruoli assegnati, decisioni approvate, evidenze tecniche e contrattuali, verifiche periodiche e capacità di intervenire quando il sistema, il contesto d’uso o la normativa cambiano.

iSimply Semplicità. Innovazione.

Visita il nostro sito
www.isimply.it

Lungo Po Antonelli, 21
10153 Torino TO
Tel +39 011 5620022
gruppo2g@gruppo2g.com

Via Palestro, 45
10015 Ivrea (TO)
Tel+39 0125 1899500
info@isimply.it

Profilo LinkedIn
di iSimply