making science

making science

AGGIORNATA AL DIGITAL OMNIBUS

Intelligenza Artificiale e AI Act: obblighi, scadenze e conseguenze per le aziende

Fabio Sutto

Una lettura ragionata delle fonti in ordine gerarchico: dal Regolamento (UE) 2024/1689 (AI Act) al Regolamento (UE) 2026/1744 (Digital Omnibus sull'IA), fino alla Legge 23 settembre 2025, n. 132 e ai suoi decreti attuativi.

Aggiornato al 10 agosto 2026

Premessa: che cosa è questo documento, e che cosa non è

Questa guida ha natura informativa e divulgativa, e serve a orientarsi prima che a decidere: l'immagine che le si addice è quella di una bussola, che dice dove ci si trova e in quale direzione conviene muoversi, mentre la rotta la traccia chi conosce l'organizzazione e risponde delle scelte che vi si compiono.

Ne discende una precisazione che non è una formula di stile: non stiamo facendo consulenza legale, non offriamo un parere professionale né assistenza in sede contenziosa, e la lettura di queste pagine non instaura alcun rapporto professionale fra chi scrive e chi legge. Le nostre valutazioni sono generali per costruzione, mentre l'applicazione del Regolamento dipende da elementi che soltanto voi conoscete: quali sistemi impiegate, con quali dati, in quale ruolo della catena del valore (fornitore, deployer, importatore, distributore) e dentro quali contratti.

Quando la sintesi e la fonte divergono prevale la fonte ufficiale: fanno fede gli atti nella versione pubblicata nella Gazzetta ufficiale dell'Unione europea (GUUE) e nella Gazzetta Ufficiale della Repubblica italiana, non il modo in cui li abbiamo riassunti qui. Al capitolo 16 trovate i riferimenti puntuali, così che ogni affermazione possa essere verificata alla fonte anziché accettata sulla fiducia.

La materia si muove mentre la si descrive, ed è la ragione per cui ogni versione porta una data in copertina; non assumiamo alcun obbligo di aggiornamento e, nei limiti consentiti dall'ordinamento, non rispondiamo delle decisioni assunte sulla base di questo documento senza una verifica riferita al caso concreto. Nei mesi che vengono l'intelligenza artificiale entrerà in un numero crescente di processi aziendali, e con essa questi obblighi: la bussola andrà riletta più di una volta.

Nella preparazione di questa guida sono stati impiegati sistemi di intelligenza artificiale, in particolare per la verifica delle fonti e del loro ordine gerarchico e per il riscontro delle risposte del capitolo 13. Ogni contenuto è stato riletto e approvato dall'autore, che ne assume la responsabilità editoriale ai sensi dell'articolo 50, paragrafo 4, dell'AI Act. La dichiarazione è volontaria: ricorrendo la revisione umana, l'obbligo non si applicherebbe.

making science

L'autore

Fabio Sutto è digital strategist, esperto di performance marketing e imprenditore digitale seriale, con oltre venticinque anni di esperienza. Ha iniziato nel 1998 come sviluppatore web e server-side, per diventare poi un riferimento in ambito SEO, Google Ads e Meta advertising e assumere infine ruoli strategici e direzionali; il suo percorso tiene insieme la competenza tecnica e l'orientamento alla crescita concreta e misurabile del business.
Come imprenditore ha fondato e fatto crescere diverse agenzie digitali. La più recente, lanciata nel 2021, si è sviluppata fino a diventare la filiale italiana del gruppo internazionale Making Science; ha inoltre contribuito alla creazione e allo sviluppo di agenzie digitali in Europa, con progetti in Irlanda, Slovenia e Croazia.
Parallelamente all'attività imprenditoriale, dal 2002 si dedica alla formazione, contribuendo alla crescita di centinaia di professionisti nel digital marketing e nella strategia. Ha tenuto corsi e docenze per istituzioni di primo piano come Luiss, Talent Garden, LVenture Group e Ninja Marketing, ed è relatore ricorrente in eventi e conferenze di settore a livello internazionale.

Making Science

Making Science Group è una società di consulenza di marketing e tecnologia che accompagna le imprese nell'accelerazione delle proprie capacità digitali. Conta oltre 1.200 professionisti distribuiti in ventidue uffici e quindici Paesi, e opera su tre linee di attività: digital marketing e adtech; cloud, software, intelligenza artificiale e cybersicurezza; Raising Tech, la divisione tecnologica. La partnership con i principali attori tecnologici del settore consente una visione completa dell'ecosistema digitale, che è il presupposto per orientarsi in una materia, come quella regolata dall'AI Act, che attraversa contemporaneamente il marketing, i dati e l'infrastruttura.
L'offerta copre l'intero ciclo di vita di una soluzione, dalla consulenza allo sviluppo, dall'integrazione alla manutenzione, con una rete globale di delivery hub che assicura scalabilità e continuità ai progetti. È un impianto che conta, quando la conformità smette di essere un adempimento documentale e diventa una questione di come i sistemi sono costruiti, addestrati e sorvegliati.
Fondata nel 2016 con una prima fase di crescita in Spagna e Portogallo, la società ha avviato nel 2020 la seconda fase con la quotazione su BME Growth ed Euronext, consolidando la presenza internazionale nei principali mercati europei. La terza fase, delineata nel "Piano 2027", è segnata dalla crescita organica negli Stati Uniti e dal consolidamento del ruolo di Google Reseller in quel mercato: Making Science è uno dei tredici Google Full Stack Sales Partner e l'unico a fornire undici servizi certificati.
Sul versante della responsabilità d'impresa, il gruppo aderisce al Climate Pledge, al Global Compact delle Nazioni Unite e all'iniziativa Pledge 1%, e il sistema di gestione ambientale delle sedi di Madrid e Chicago è certificato Bureau Veritas secondo le norme ISO 14001, ISO 9001 e ISO 27001.

In sintesi: le cinque cose da sapere

1. Una parte degli obblighi è già in vigore. Dal 2 agosto 2026 si applicano gli obblighi di trasparenza: dichiarare che si sta interagendo con un'intelligenza artificiale, marcare i contenuti generati o manipolati artificialmente, informare chi è esposto a sistemi biometrici. Le autorità di vigilanza hanno pieni poteri ispettivi e sanzionatori.

2. La parte più pesante è stata rinviata, non cancellata. Gli obblighi sui sistemi ad alto rischio slittano al 2 dicembre 2027 e al 2 agosto 2028. I tempi tecnici di adeguamento sono di dodici-diciotto mesi.

3. Le scadenze da segnare.

Data	Che cosa succede
già in vigore	Divieti sulle pratiche vietate, obblighi sui modelli per finalità generali, obblighi di trasparenza, vigilanza e sanzioni
10 ottobre 2026	Termine per i decreti attuativi della legge italiana sull'IA
2 dicembre 2026	Nuovi divieti su deepfake sessuali non consensuali; marcatura obbligatoria per i sistemi generativi già sul mercato
9 dicembre 2026	Nuova disciplina della responsabilità da prodotto difettoso: software e IA sono prodotti
2 dicembre 2027	Obblighi sui sistemi ad alto rischio dell'Allegato III (personale, credito, istruzione, biometria)
2 agosto 2028	Obblighi sui sistemi ad alto rischio incorporati in prodotti regolati

4. Quanto si rischia. Fino a 35 milioni di euro o al 7% del fatturato mondiale per le pratiche vietate; fino a 15 milioni o al 3% per la violazione degli altri obblighi, compresa la trasparenza; fino a 7,5 milioni o all'1% per informazioni inesatte alle autorità. Per le PMI si applica l'importo inferiore fra i due. A queste si sommano le sanzioni del Garante privacy, che sono il canale oggi più attivo, e il rischio di cause civili.

5. Tre cose da fare subito. Fare l'inventario dei sistemi di intelligenza artificiale realmente in uso, compresi quelli adottati dalle singole funzioni senza passare dall'IT. Verificare di non impiegare pratiche vietate, a partire dall'analisi delle emozioni dei dipendenti. Controllare che chatbot, contenuti generati e comunicazioni automatizzate dichiarino quello che devono dichiarare.

Se avete poco tempo
Il capitolo 6 spiega che cosa è già obbligatorio, il capitolo 8 traduce gli obblighi per tipo di azienda, il capitolo 12 dice da dove cominciare e il capitolo 13 risponde alle domande che nascono applicandoli. Gli altri capitoli servono a capire perché.

making science

Indice

1. Perché questo documento, e perché adesso

Il 2 agosto 2026 è la data che il legislatore europeo aveva indicato fin dal 2024 come momento di "applicazione generale" del Regolamento sull'intelligenza artificiale, e la scadenza non ha nulla di simbolico: da quel giorno le autorità nazionali di vigilanza dispongono di pieni poteri ispettivi e sanzionatori; sono inoltre diventati esigibili alcuni obblighi che riguardano potenzialmente ogni impresa, e non soltanto quelle tecnologiche.

Nelle settimane immediatamente precedenti il quadro è però cambiato, in quanto il Regolamento (UE) 2026/1744, il cosiddetto "Digital Omnibus sull'intelligenza artificiale", pubblicato nella Gazzetta ufficiale dell'Unione europea del 24 luglio 2026 ed entrato in vigore il 27 luglio 2026, ha rinviato di oltre un anno la parte più onerosa della disciplina, quella sui sistemi ad alto rischio; ne risulta un quadro a due velocità, che si presta con facilità a due errori speculari e ugualmente costosi.

I due errori da evitare
Il primo consiste nel ritenere che, poiché "tanto è tutto rinviato", non ci sia nulla da fare; dal 2 agosto 2026 sono invece pienamente applicabili gli obblighi di trasparenza, il regime sanzionatorio e la vigilanza del mercato.
Il secondo sta all'estremo opposto, e consiste nell'avviare oggi un progetto di conformità dimensionato sugli obblighi da "alto rischio", sostenendo così costi che il calendario consentirebbe di distribuire su due anni.

Questa guida serve a distinguere le due cose. Prende le mosse dalle fonti, disposte secondo la gerarchia che decide chi comanda su cosa, e arriva agli adempimenti concreti, differenziati secondo il ruolo che l'impresa svolge: chi usa strumenti di IA acquistati da terzi, chi li sviluppa o li rivende, chi produce modelli di base, chi opera nel settore pubblico.
Non diamo nulla per scontato: ogni concetto tecnico è spiegato la prima volta che compare, e un glossario finale raccoglie i termini ricorrenti.

2. La gerarchia delle fonti: chi comanda su cosa

Quando si parla di "regole sull'intelligenza artificiale" si mescolano con facilità atti di rango profondamente diverso, e dalla loro distinzione dipendono tre cose concrete: che cosa è vincolante, che cosa è soltanto interpretativo, quale norma prevale in caso di contrasto. Procediamo quindi dall'alto verso il basso.

2.1 Il vertice: diritto primario dell'Unione

Al livello più alto si collocano i Trattati (TUE e TFUE) e la Carta dei diritti fondamentali dell'Unione europea; l'AI Act si fonda sull'articolo 114 TFUE (ravvicinamento delle legislazioni per il mercato interno) e sull'articolo 16 TFUE (protezione dei dati personali). Quanto alla Carta, la dignità umana, la non

discriminazione, la vita privata e la libertà d'impresa sono i parametri con cui i giudici leggeranno i casi concreti, e sono la ragione per cui alcune pratiche sono state vietate in assoluto.

2.2 I regolamenti e le direttive dell'Unione

Le fonti europee di questo livello sono di due tipi, e la differenza conta. Il regolamento si applica direttamente in ogni Stato membro, senza bisogno di una legge nazionale: è il caso dell'AI Act, e per questo il 2 agosto 2026 è scattato lo stesso giorno a Milano come a Lisbona. La direttiva fissa invece un risultato da raggiungere e lascia a ciascuno Stato il compito di recepirla entro un termine: fino a quel momento, e salvo eccezioni, l'impresa risponde alla norma nazionale vigente. Nella tabella che segue, pertanto, l'ultima riga ha una logica diversa dalle altre: indica scadenze di recepimento, non date di applicazione.

Atto	Che cosa disciplina	Rilievo per l'impresa
Regolamento (UE) 2024/1689, AI Act	Il testo base: definizioni, pratiche vietate, sistemi ad alto rischio, obblighi di trasparenza, modelli per finalità generali, governance, sanzioni.	È la norma madre. Entrato in vigore il 1° agosto 2024, si applica per fasi successive.
Regolamento (UE) 2026/1744, Digital Omnibus sull'IA	Modifica l'AI Act: rinvia gli obblighi sull'alto rischio, semplifica alcuni adempimenti, introduce due nuovi divieti.	Non sostituisce l'AI Act: lo emenda. Va letto insieme, non al posto, del testo del 2024.
Regolamento (UE) 2016/679, GDPR	Trattamento dei dati personali.	Continua ad applicarsi integralmente. Quasi ogni sistema di IA aziendale tratta dati personali: due discipline, due valutazioni, due autorità.
Regolamento (UE) 2023/2854, Data Act	Accesso ai dati generati da prodotti connessi e servizi correlati, condivisione fra imprese, portabilità fra fornitori di servizi cloud.	Rileva per chi addestra o alimenta sistemi di IA con dati industriali o di prodotti connessi, e per le clausole di uscita dai contratti cloud.
Regolamenti settoriali di prodotto	Dispositivi medici (2017/745), macchine (2023/1230), giocattoli, sicurezza generale dei prodotti (2023/988).	Se il vostro prodotto è già regolato e incorpora IA, le due discipline si sommano e si coordinano (Allegato I dell'AI Act).
Regolamento (UE) 2022/2065, DSA	Piattaforme online e moderazione dei contenuti.	Rileva per marketplace, social e servizi di intermediazione che usano sistemi di raccomandazione.
Direttive dell'Unione (da recepire)	Direttiva (UE) 2024/2853 sulla responsabilità da prodotto difettoso, che include espressamente software e sistemi di IA; direttiva (UE) 2022/2555 (NIS2) sulla cybersicurezza.	Non si applicano da sole: valgono attraverso la legge nazionale di recepimento. Per la 2024/2853 il termine è il 9 dicembre 2026 e in Italia la delega è nella legge di delegazione europea 2025.

2.3 Atti delegati, atti di esecuzione e norme armonizzate

Sotto i regolamenti si collocano gli atti con cui la Commissione europea aggiorna e specifica il quadro: atti delegati (che possono, ad esempio, modificare l'elenco dei sistemi ad alto rischio dell'Allegato III) e atti di esecuzione. Accanto a questi, le norme tecniche armonizzate elaborate da CEN-CENELEC: non sono obbligatorie, ma chi le applica beneficia di una presunzione di conformità, cioè si presume, salvo prova contraria, che rispetti i requisiti del regolamento. È il meccanismo classico del diritto europeo dei prodotti, ed è la via più efficiente per dimostrare conformità.

2.4 La soft law: linee guida e codici di buone pratiche

Questo livello non vincola in senso stretto; è però quello che le autorità useranno concretamente per valutare i comportamenti. Ignorarlo è imprudente.

- Linee guida della Commissione europea. Fra le più rilevanti: gli orientamenti sulle pratiche vietate e sulla definizione di sistema di IA (febbraio 2025), gli orientamenti sui modelli per finalità generali (luglio 2025) e, la più importante per la scadenza di agosto, gli Orientamenti sull'attuazione dell'articolo 50 in materia di trasparenza, pubblicati il 20 luglio 2026.
- Codici di buone pratiche. Il Codice per i modelli GPAI (luglio 2025) e il Codice di buone pratiche sulla trasparenza dei contenuti generati dall'IA (10 giugno 2026). L'adesione è volontaria; la Commissione ha però chiarito che aderirvi è il modo più semplice per dimostrare la conformità agli obblighi di trasparenza, che restano invece giuridicamente vincolanti.
- Standard di gestione. Il regolamento non richiama la norma ISO/IEC 42001 (sistema di gestione dell'intelligenza artificiale), che offre però un'ossatura organizzativa riconosciuta e certificabile, utile soprattutto nelle gare e nelle due diligence.

2.5 Il livello nazionale italiano

Un regolamento europeo non ha bisogno di recepimento, ma lascia agli Stati membri alcuni spazi obbligati: designare le autorità, disciplinare i procedimenti sanzionatori, istituire gli spazi di sperimentazione. L'Italia ha scelto di fare qualcosa di più, adottando una legge di sistema.

Fonte	Contenuto	Stato
Legge 23 settembre 2025, n. 132	Prima legge nazionale organica sull'IA: principi, settori (sanità, lavoro, professioni, PA, giustizia), governance, deleghe al Governo, nuove fattispecie penali.	In vigore dal 10 ottobre 2025.
Decreti legislativi attuativi	Poteri delle autorità, vigilanza e sanzioni, sandbox regolamentare, formazione e lavoro; uso dell'IA in ambito di polizia, responsabilità civile e penale.	Approvati in esame preliminare dal Consiglio dei Ministri il 10 giugno 2026; iter in corso. Il termine della delega scade il 10 ottobre 2026.
Norme preesistenti incise dalla legge	Art. 1-bis del D.Lgs. 152/1997 (informativa ai lavoratori su sistemi decisionali automatizzati); legge 633/1941 sul diritto d'autore (tutela riservata alla creazione umana; nuova disciplina sull'estrazione di testi e	In vigore.

Fonte	Contenuto	Stato
	dati); Codice penale (nuovo reato di diffusione illecita di contenuti generati con IA; aggravante comune).	
Provvedimenti delle autorità	Atti di ACN, AgID, Garante privacy, Banca d'Italia, CONSOB, IVASS nei rispettivi ambiti.	In progressiva adozione.

Una precisazione importante sulla gerarchia
La legge italiana non può derogare al regolamento europeo né ridurne la portata: può solo integrarlo negli spazi che il regolamento stesso lascia agli Stati. Dove le due discipline si sovrappongono, prevale il diritto dell'Unione. In pratica, per l'impresa questo significa che il primo riferimento resta sempre l'AI Act; la legge 132/2025 aggiunge obblighi ulteriori, in particolare informativi, che valgono solo in Italia.

3. Prima domanda: che ruolo avete?

L'AI Act non impone gli stessi obblighi a tutti, ma li distribuisce lungo la catena del valore secondo il ruolo che ciascun soggetto svolge rispetto a un determinato sistema, e la stessa azienda può ritrovarsi con ruoli diversi per sistemi diversi. Identificare il ruolo è quindi il primo adempimento, perché tutto il resto ne discende.

3.1 I cinque ruoli della catena del valore

Ruolo	Definizione (art. 3 AI Act)	Esempio concreto
Fornitore (provider)	Chi sviluppa un sistema di IA, o lo fa sviluppare, e lo immette sul mercato o lo mette in servizio con il proprio nome o marchio, a titolo oneroso o gratuito.	Una software house che vende un gestionale con funzioni di IA. Ma anche l'azienda che sviluppa internamente uno strumento e lo mette in servizio per uso proprio.
Deployer (utilizzatore/deployer)	Chi utilizza un sistema di IA sotto la propria autorità, nell'ambito di un'attività professionale.	Lo studio che usa un assistente di scrittura; l'azienda che adotta un software di screening dei curricula; la banca che impiega un modello di scoring.
Importatore	Chi immette sul mercato UE un sistema di un fornitore stabilito fuori dall'Unione.	L'azienda italiana che porta sul mercato europeo una soluzione statunitense.
Distributore	Chi mette a disposizione sul mercato un sistema senza esserne fornitore o importatore.	Il rivenditore o l'integratore che commercializza software di terzi.
Fornitore di modelli GPAI	Chi sviluppa un modello di IA per finalità generali (i grandi modelli linguistici e multimodali).	Gli sviluppatori dei modelli di base. Riguarda pochissime imprese, ma con obblighi molto stringenti.

3.2 Quando si diventa fornitori senza accorgersene: l'articolo 25

Il ruolo non è una scelta: dipende da quello che si fa, non da come ci si definisce. L'articolo 25 dell'AI Act stabilisce infatti che un deployer, un distributore o un importatore assume gli obblighi del fornitore in tre casi: se appone il proprio nome o marchio su un sistema già immesso sul mercato; se apporta una modifica sostanziale a un sistema; se ne modifica la finalità prevista in modo tale da farlo rientrare fra i sistemi ad alto rischio.
È un passaggio che nella pratica si verifica di frequente. Pensiamo al chatbot di un fornitore terzo, personalizzato con i contenuti aziendali e presentato al pubblico con il proprio marchio: agli occhi del

regolamento quell'impresa non è più soltanto un utilizzatore. Il rischio è di trovarsi con gli obblighi del produttore senza disporre della documentazione tecnica del modello sottostante, documentazione che solo il fornitore originario possiede.

Il punto pratico
È un problema che si risolve in sede contrattuale, prima che tecnica. Chi personalizza o rimarchia un sistema di terzi deve quindi verificare che il contratto garantisca l'accesso alla documentazione necessaria e definisca chi risponde di che cosa. Torniamo su questo punto nel capitolo 8.

4. La logica del regolamento: quattro livelli di rischio

L'AI Act non regola la tecnologia in sé, ma l'uso che se ne fa, tanto che lo stesso algoritmo può risultare irrilevante in un contesto e severamente regolato in un altro. La classificazione avviene quindi su quattro livelli.

4.1 Rischio inaccettabile: le pratiche vietate

L'articolo 5 elenca le pratiche vietate in assoluto, applicabili dal 2 febbraio 2025. Fra queste: le tecniche manipolative o subliminali che distorcono materialmente il comportamento causando un danno significativo; lo sfruttamento delle vulnerabilità legate a età, disabilità o situazione socioeconomica; il punteggio sociale (social scoring); la valutazione predittiva del rischio che una persona commetta un reato basata unicamente sulla profilazione; la creazione di banche dati di riconoscimento facciale mediante scraping non mirato; il riconoscimento delle emozioni sul luogo di lavoro e negli istituti di istruzione; la categorizzazione biometrica per dedurre dati sensibili; l'identificazione biometrica remota in tempo reale in spazi accessibili al pubblico a fini di attività di contrasto, salvo eccezioni tassative.
Due pratiche vietate riguardano da vicino le imprese ordinarie: il riconoscimento delle emozioni dei dipendenti (software che analizzano espressioni facciali o tono di voce per valutare coinvolgimento, stress o produttività) e la categorizzazione biometrica che deduce convinzioni politiche o religiose, orientamento sessuale, appartenenza sindacale. Sono vietati a prescindere dal consenso dell'interessato.
Il Digital Omnibus ha aggiunto due nuovi divieti, applicabili dal 2 dicembre 2026: l'uso di sistemi di IA per generare o manipolare, senza consenso, immagini o video intimi realistici di persone identificabili, e la generazione di materiale pedopornografico.

4.2 Rischio alto

Due strade portano alla qualifica di alto rischio. La prima (articolo 6, paragrafo 1, e Allegato I): il sistema è un componente di sicurezza di un prodotto già soggetto a normativa europea di armonizzazione (dispositivi medici, macchine, ascensori, giocattoli, veicoli) e quel prodotto è sottoposto a valutazione di conformità da parte di terzi. La seconda (articolo 6, paragrafo 2, e Allegato III): il sistema è destinato a uno degli otto ambiti elencati, fra cui biometria, infrastrutture critiche, istruzione e formazione professionale, occupazione e gestione dei lavoratori, accesso a servizi essenziali pubblici e privati (incluso il merito creditizio e la determinazione dei premi assicurativi vita e salute), attività di contrasto, migrazione e asilo, amministrazione della giustizia.
Esiste un filtro: un sistema che rientrerebbe nell'Allegato III non è considerato ad alto rischio se svolge soltanto compiti procedurali limitati, migliora il risultato di un'attività umana già completata, rileva schemi decisionali senza sostituire la valutazione umana, o svolge compiti puramente preparatori. Chi invoca l'esclusione deve però documentare la valutazione prima dell'immissione sul mercato e registrarsi nella banca dati europea. La deroga non opera mai se il sistema effettua profilazione di persone fisiche.

Il Digital Omnibus ha aggiunto ulteriori esclusioni per i sistemi dell'Allegato I: restano fuori quelli usati esclusivamente per funzioni non connesse alla sicurezza, come l'assistenza all'utente, l'ottimizzazione delle prestazioni o il controllo qualità di aspetti non legati alla sicurezza.

4.3 Rischio limitato: gli obblighi di trasparenza

È il livello che riguarda il maggior numero di imprese, ed è quello diventato applicabile il 2 agosto 2026. Non impone certificazioni né sistemi di gestione del rischio: impone di dire come stanno le cose. Vi dedichiamo il capitolo 6, dopo aver messo in fila le date nel capitolo 5.

4.4 Rischio minimo

Tutto il resto: filtri antispam, correttori ortografici, sistemi di raccomandazione di base, IA nei videogiochi. Non c'è alcun obbligo specifico, salvo l'invito ad adottare volontariamente codici di condotta, e restano naturalmente applicabili le altre discipline, a partire dal GDPR.

4.5 I modelli per finalità generali (GPAI): una categoria a parte

I modelli di IA per finalità generali sono regolati in modo autonomo, perché non hanno una destinazione d'uso predefinita. Gli obblighi dell'articolo 53 si applicano dal 2 agosto 2025 e comprendono: documentazione tecnica del modello; informazioni ai fornitori a valle che lo integrano nei propri sistemi; una politica di rispetto del diritto d'autore; una sintesi sufficientemente dettagliata dei contenuti usati per l'addestramento, secondo il modello pubblicato dalla Commissione. Per i modelli con rischio sistemico (presunti tali oltre una soglia di potenza di calcolo) si aggiungono valutazione avversariale, mitigazione dei rischi, segnalazione degli incidenti gravi e protezione della cybersicurezza.

5. Il calendario completo, aggiornato dopo il Digital Omnibus

La tabella che segue è la mappa temporale da tenere davanti. Le scadenze fino al 2 agosto 2026 sono già decorse; le successive arrivano fino al 31 dicembre 2030.

Data	Che cosa diventa applicabile	Riferimento
1° agosto 2024	Entrata in vigore dell'AI Act. Nessun obbligo immediato: inizia a decorrere il calendario.	Art. 113 Reg. (UE) 2024/1689
2 febbraio 2025	Capo I e Capo II: definizioni e ambito di applicazione; obbligo di alfabetizzazione in materia di IA (art. 4); divieto delle pratiche vietate (art. 5).	Art. 113, lett. a)
2 agosto 2025	Capo V (modelli GPAI); Capo VII (governance europea e nazionale); Capo XII (sanzioni), con l'eccezione dell'art. 101; art. 78 (riservatezza). Termine per la designazione delle autorità nazionali.	Art. 113, lett. b)
10 ottobre 2025	Entrata in vigore della legge italiana n. 132/2025: principi nazionali, obblighi informativi, nuove fattispecie penali.	L. 23 settembre 2025, n. 132
27 luglio 2026	Entrata in vigore del Digital Omnibus sull'IA, che modifica il calendario e alcuni obblighi.	Reg. (UE) 2026/1744
2 agosto 2026	Data di applicazione generale. Obblighi di trasparenza (art. 50); ammende della Commissione ai fornitori di modelli GPAI (art. 101); piena operatività della vigilanza del mercato e del regime sanzionatorio nazionale; spazi di sperimentazione normativa operativi negli Stati membri.	Art. 113 Reg. 2024/1689
2 dicembre 2026	Nuovi divieti su deepfake sessuali non consensuali e materiale pedopornografico generato con IA. Termine per adeguare alla marcatura tecnica i sistemi generativi già immessi sul mercato prima del 2 agosto 2026.	Reg. (UE) 2026/1744; art. 111, par. 4
2 agosto 2027	Fine del periodo transitorio per i modelli GPAI immessi sul mercato prima del 2 agosto 2025.	Art. 111, par. 3
2 dicembre 2027	Obblighi sui sistemi ad alto rischio dell'Allegato III (art. 6, par. 2): gestione del rischio, governo dei dati, documentazione, sorveglianza umana, registrazione, valutazione d'impatto sui diritti fondamentali.	Reg. (UE) 2026/1744 (termine originario: 2 agosto 2026)
2 agosto 2028	Obblighi sui sistemi ad alto rischio dell'Allegato I, cioè l'IA incorporata in prodotti già regolati (dispositivi medici, macchine, giocattoli).	Reg. (UE) 2026/1744 (termine originario: 2 agosto 2027)

Data	Che cosa diventa applicabile	Riferimento
2 agosto 2030	Sistemi ad alto rischio destinati all'uso da parte di autorità pubbliche immessi sul mercato prima delle rispettive date di applicazione.	Art. 111, par. 2
31 dicembre 2030	Componenti di IA nei sistemi IT su larga scala dell'Allegato X (settore libertà, sicurezza e giustizia).	Art. 111, par. 1

6. Che cosa è scattato il 2 agosto 2026

Il 2 agosto 2026 sono entrati in funzione tre blocchi di natura diversa: gli obblighi sostanziali di trasparenza, i poteri di enforcement e gli strumenti di supporto.

6.1 Gli obblighi di trasparenza (articolo 50)

È la parte che tocca il numero più ampio di imprese, incluse quelle che non sviluppano nulla e si limitano a usare strumenti disponibili sul mercato, e la logica che la governa è semplice: le persone hanno diritto di sapere quando stanno parlando con una macchina e quando un contenuto è artificiale. Gli obblighi sono quattro, e si distribuiscono fra fornitori e deployer.

Norma	Chi è obbligato	Che cosa deve fare
Art. 50, par. 1	Il fornitore del sistema	Progettare i sistemi destinati a interagire direttamente con le persone in modo che sia chiaro che si sta interagendo con un'IA. L'obbligo non si applica se la circostanza è evidente per una persona ragionevolmente informata e attenta.
Art. 50, par. 2	Il fornitore del sistema, compresi i fornitori di modelli GPAI	Marcare i contenuti sintetici (audio, immagini, video, testo) in formato leggibile meccanicamente e renderli rilevabili come generati o manipolati artificialmente: filigrane, metadati, identificativi crittografici. Le soluzioni devono essere efficaci, interoperabili, robuste e affidabili.
Art. 50, par. 3	Il deployer	Informare le persone esposte del funzionamento di sistemi di riconoscimento delle emozioni o di categorizzazione biometrica, e trattarne i dati nel rispetto del GDPR. Si ricordi che nei luoghi di lavoro e nell'istruzione il riconoscimento delle emozioni è comunque vietato.
Art. 50, par. 4	Il deployer	Rendere noto che un contenuto è un deepfake, cioè generato o manipolato artificialmente. Per i testi pubblicati allo scopo di informare il pubblico su questioni di interesse pubblico, dichiarare che sono generati artificialmente, salvo che il contenuto sia stato sottoposto a revisione umana con assunzione di responsabilità editoriale.

Le informazioni devono essere fornite in modo chiaro e distinguibile al più tardi al momento della prima interazione o esposizione. Per i contenuti manifestamente artistici, creativi, satirici o di finzione l'obbligo è attenuato, in quanto va assolto con modalità che non ostacolino la fruizione dell'opera: tipicamente nei

titoli di coda o in una nota, non con una scritta sovrimpressa. Questi obblighi sono quelli che nella pratica sollevano il maggior numero di domande, dal perimetro di ciò che va dichiarato alle parole da usare: il capitolo 13 le raccoglie e vi risponde caso per caso.

Gli orientamenti della Commissione del 20 luglio 2026
Poche settimane prima della scadenza, la Commissione europea ha pubblicato le linee guida sull'attuazione dell'articolo 50, accompagnate dal Codice di buone pratiche sulla trasparenza dei contenuti generati dall'IA, del 10 giugno 2026. Il Codice, elaborato da esperti indipendenti con il contributo degli stakeholder, è riconosciuto come strumento volontario idoneo a dimostrare la conformità.
Per un'impresa la conseguenza pratica è duplice: l'adesione al Codice offre un porto sicuro reputazionale e probatorio; la mancata adesione non costituisce di per sé una violazione, ma impone di dimostrare in altro modo l'adeguatezza delle misure adottate.

6.2 Il regime sanzionatorio e la vigilanza

Il Capo XII sulle sanzioni si applica dal 2 agosto 2025, con l'unica eccezione dell'articolo 101 (le ammende che la Commissione può irrogare direttamente ai fornitori di modelli GPAI), che decorre dal 2 agosto 2026. Ma è da quest'ultima data che il sistema diventa realmente operativo: le autorità nazionali di vigilanza del mercato esercitano pieni poteri di controllo, richiesta di informazioni, ispezione e adozione di misure correttive, e l'Ufficio per l'IA della Commissione può agire sui fornitori di modelli.

6.3 Gli spazi di sperimentazione normativa

Dal 2 agosto 2026 ogni Stato membro deve avere operativo almeno uno spazio di sperimentazione normativa (regulatory sandbox), previsto dall'articolo 57: un ambiente controllato in cui sviluppare e testare sistemi innovativi sotto la supervisione dell'autorità, con orientamenti e, soprattutto, con una ragionevole prevedibilità sulle conseguenze. In Italia lo schema di decreto attuativo affida la sandbox nazionale alla gestione congiunta di AgID e ACN. Per le PMI è una leva che vale la pena valutare, anche perché l'accesso è previsto in via prioritaria e gratuita.

7. Che cosa è stato rinviato, e perché non è un "liberi tutti"

Il Digital Omnibus ha spostato in avanti l'intero pacchetto sui sistemi ad alto rischio, cioè le sezioni 1, 2 e 3 del Capo III: la gestione del rischio, la governance dei dati, la documentazione tecnica, la registrazione degli eventi, la sorveglianza umana, l'accuratezza e la cybersicurezza, la valutazione della conformità e la marcatura CE, la registrazione nella banca dati europea, la valutazione d'impatto sui diritti fondamentali.

Categoria	Termine originario	Nuovo termine
Sistemi ad alto rischio dell'Allegato III (selezione del personale, credito, istruzione, biometria, servizi essenziali)	2 agosto 2026	2 dicembre 2027
Sistemi ad alto rischio dell'Allegato I (IA incorporata in prodotti regolati: dispositivi medici, macchine, giocattoli)	2 agosto 2027	2 agosto 2028

Il rinvio nasce da una ragione pratica riconosciuta apertamente dalle istituzioni: le norme tecniche armonizzate che dovevano rendere concreti quei requisiti non erano pronte. Chiedere alle imprese di conformarsi a requisiti privi di specifiche tecniche avrebbe generato incertezza senza aumentare la tutela.

7.1 Le semplificazioni introdotte

- Alfabetizzazione in materia di IA. L'obbligo dell'articolo 4 è stato riformulato: non è più richiesto a fornitori e deployer di garantire uno specifico livello di competenza del personale, ma di adottare misure adeguate a promuoverne la formazione, con il supporto della Commissione e degli Stati membri. È un alleggerimento pensato per le realtà più piccole. Resta però un fatto: la formazione documentata è la prima cosa che un'autorità chiede di vedere, ed è anche la difesa più economica.
- Registrazione nella banca dati europea. Semplificata per i sistemi a rischio limitato: le informazioni richieste sono ridotte e razionalizzate. L'adempimento resta, ma è più leggero.
- Trattamento dei dati per la correzione dei bias. Il nuovo articolo 4-bis consente in via eccezionale ai fornitori di sistemi ad alto rischio di trattare categorie particolari di dati personali per rilevare e correggere le distorsioni, a condizioni rigorose (pseudonimizzazione, cancellazione dopo la correzione). Le garanzie del GDPR restano applicabili.
- Piccole imprese a media capitalizzazione. È stata introdotta una categoria intermedia fra PMI e grandi imprese, per le aziende che hanno superato le soglie dimensionali delle PMI ma ne condividono i vincoli organizzativi. Le sanzioni pecuniarie devono tenere conto della loro sostenibilità economica.

7.2 L'altro Digital Omnibus, quello sui dati: che cosa aspettarsi

Una precisazione serve a evitare un equivoco ricorrente: il pacchetto di semplificazione presentato dalla Commissione nel novembre 2025 era doppio, cioè due proposte distinte, presentate insieme e spesso confuse fra loro. La prima riguardava l'intelligenza artificiale ed è quella di cui abbiamo parlato finora, diventata il Regolamento (UE) 2026/1744. La seconda riguarda i dati, ha seguito un percorso più lento ed è tuttora all'esame del Consiglio.
Quando si legge che "il Digital Omnibus è stato approvato", quindi, ci si riferisce solo alla metà che riguarda l'IA. L'altra metà è ancora una proposta, e nulla di ciò che segue è oggi diritto vigente.
Vale però la pena sapere che cosa c'è dentro, perché tocca proprio i punti di contatto fra intelligenza artificiale e protezione dei dati:

- una nuova definizione di dato personale, con effetti a catena sull'intero perimetro di applicazione del GDPR;
- il chiarimento che lo sviluppo e il miglioramento dei sistemi di IA possono fondarsi sul legittimo interesse, che è oggi la questione più discussa in materia di addestramento dei modelli;
- nuove eccezioni per i dati biometrici e le categorie particolari di dati;
- una revisione del regime di notifica delle violazioni dei dati personali;
- interventi su ePrivacy e sulla NIS2, e il riassorbimento nel Data Act di Data Governance Act, direttiva Open Data e regolamento sul libero flusso dei dati non personali.

Il percorso non è pacifico: il Comitato europeo per la protezione dei dati e il Garante europeo hanno adottato nel febbraio 2026 un parere congiunto critico, e il testo ha continuato a cambiare nei lavori del Consiglio.

Che cosa farne, in pratica
Nulla di tutto questo va anticipato: costruire oggi una strategia su una proposta che può ancora cambiare è un errore. Due indicazioni concrete però esistono.
Se state valutando di addestrare o affinare modelli su dati personali, la base giuridica su cui vi state interrogando è esattamente ciò che si sta discutendo a Bruxelles. Questo non autorizza ad aspettare, ma consiglia di documentare bene la scelta fatta oggi (valutazione del legittimo interesse, bilanciamento, misure di garanzia), così che un eventuale cambio di quadro trovi una posizione motivata e non un vuoto.
Se avete progetti in cantiere che dipendono da questi punti, vale la pena inserire il monitoraggio del dossier fra le attività ricorrenti, con una verifica ogni trimestre.

7.3 Perché conviene comunque muoversi ora

Il rinvio riguarda la data di esigibilità degli obblighi, non la loro esistenza. Tre ragioni concrete sconsigliano di rinviare a propria volta:

- I tempi tecnici sono lunghi. Costruire un sistema di gestione del rischio, ricostruire la provenienza e la qualità dei dati di addestramento, predisporre la documentazione tecnica e, dove serve, passare attraverso un organismo notificato richiede tipicamente dodici-diciotto mesi. Dicembre 2027 non è lontano quanto sembra.
- Il mercato corre più veloce della legge. Nei contratti B2B e nelle gare pubbliche le dichiarazioni di conformità all'AI Act sono già oggi requisito di partecipazione o clausola negoziata. La conformità anticipata è un argomento commerciale prima che un adempimento.
- Gli obblighi già applicabili non sono sospesi. Divieti, trasparenza, GPAI, obblighi nazionali della legge 132/2025: tutto questo è pienamente esigibile oggi, e la vigilanza è operativa.

8. Gli obblighi, azienda per azienda

Questa sezione traduce il quadro normativo in adempimenti, distinti per tipologia di impresa, e molte organizzazioni si riconosceranno in più di un profilo.

8.1 L'azienda che usa strumenti di IA acquistati da terzi (deployer)

È la situazione più diffusa: assistenti conversazionali, strumenti di generazione testi e immagini, software di analisi documentale, moduli di IA integrati nel gestionale o nel CRM.

Obblighi già esigibili oggi

- Non utilizzare pratiche vietate. In particolare: niente analisi delle emozioni dei dipendenti tramite espressioni facciali, tono di voce o parametri biometrici; niente categorizzazione biometrica per dedurre dati sensibili.
- Promuovere l'alfabetizzazione del personale che usa i sistemi (art. 4). Formazione proporzionata al ruolo, documentata e ripetuta nel tempo.
- Trasparenza verso il pubblico. Se usate un chatbot sul sito, deve essere chiaro che è un'IA; i contenuti generati o manipolati artificialmente vanno dichiarati, e lo stesso vale per i testi su questioni di interesse pubblico generati dall'IA, salvo revisione umana con responsabilità editoriale. I casi concreti, comprese le campagne e i contenuti organici sui social, sono al capitolo 13.
- Informativa ai lavoratori e alle rappresentanze sindacali sull'uso di sistemi decisionali o di monitoraggio automatizzati (legge 132/2025 e art. 1-bis del D.Lgs. 152/1997).
- Informativa alla clientela quando l'IA è impiegata nell'erogazione di prestazioni professionali o di servizi.
- Conformità al GDPR, che viaggia in parallelo per tutta la durata del progetto: base giuridica, informativa, valutazione d'impatto, decisioni automatizzate. Il rapporto fra le due discipline è trattato al § 10.1.

Da preparare per il 2 dicembre 2027 (se usate sistemi che saranno classificati ad alto rischio)

- Utilizzare il sistema conformemente alle istruzioni per l'uso del fornitore.
- Assicurare una sorveglianza umana effettiva, affidata a persone competenti e dotate dell'autorità di intervenire.
- Verificare la pertinenza e la rappresentatività dei dati di input che controllate.
- Conservare i log generati automaticamente, di regola per almeno sei mesi.
- Informare i lavoratori interessati prima della messa in servizio di un sistema ad alto rischio sul luogo di lavoro.
- Informare le persone fisiche sottoposte a decisioni che le riguardano, e garantire il diritto a una spiegazione sul ruolo del sistema.
- Sospendere l'uso e informare fornitore e autorità in caso di rischio o incidente grave.
- Per gli organismi pubblici e alcuni soggetti privati che erogano servizi essenziali: valutazione d'impatto sui diritti fondamentali (FRIA).

8.2 L'azienda che sviluppa, personalizza o rivende sistemi di IA (fornitore)

Obblighi già esigibili oggi

- Progettare i sistemi che interagiscono con le persone in modo che l'interazione con l'IA sia riconoscibile (art. 50, par. 1).
- Implementare la marcatura tecnica dei contenuti sintetici: filigrane, metadati o identificativi leggibili meccanicamente (art. 50, par. 2). Per i sistemi generativi già sul mercato prima del 2 agosto 2026, il termine di adeguamento è il 2 dicembre 2026.
- Assicurarsi che i sistemi non realizzino pratiche vietate, incluse quelle aggiunte dal Digital Omnibus dal 2 dicembre 2026.
- Governare la catena di fornitura: se integrate modelli o componenti di terzi, procuratevi la documentazione che vi servirà per i vostri obblighi.

Da preparare per il 2 dicembre 2027 / 2 agosto 2028

- Sistema di gestione dei rischi lungo l'intero ciclo di vita del sistema.
- Governance dei dati: qualità, pertinenza, rappresentatività dei set di addestramento, convalida e prova; esame delle possibili distorsioni.
- Documentazione tecnica completa e istruzioni per l'uso destinate ai deployer.
- Registrazione automatica degli eventi (logging) e tracciabilità.
- Progettazione che consenta una sorveglianza umana effettiva.
- Livelli adeguati di accuratezza, robustezza e cybersicurezza.
- Sistema di gestione della qualità documentato.
- Valutazione della conformità, dichiarazione UE di conformità, marcatura CE.
- Registrazione del sistema nella banca dati europea prima dell'immissione sul mercato.
- Monitoraggio successivo alla commercializzazione e segnalazione degli incidenti gravi.
- Rappresentante autorizzato nell'Unione, per i fornitori stabiliti in Paesi terzi.

8.3 I fornitori di modelli per finalità generali (GPAI)

Obblighi applicabili dal 2 agosto 2025; per i modelli già immessi sul mercato prima di quella data, l'adeguamento va completato entro il 2 agosto 2027. Dal 2 agosto 2026 la Commissione può irrogare ammende dirette.

- Documentazione tecnica del modello, aggiornata e disponibile su richiesta dell'Ufficio per l'IA.
- Informazioni e documentazione ai fornitori a valle che integrano il modello nei propri sistemi.
- Politica di conformità alla normativa sul diritto d'autore, incluso il rispetto delle riserve di estrazione di testo e dati.
- Sintesi sufficientemente dettagliata dei contenuti utilizzati per l'addestramento, secondo il modello pubblicato dalla Commissione.
- Per i modelli con rischio sistemico: valutazione del modello con test avversariali, mitigazione dei rischi sistemici, segnalazione degli incidenti gravi, protezione della cybersicurezza del modello e dell'infrastruttura fisica.

8.4 Importatori e distributori

- Verificare, prima di immettere sul mercato, che il fornitore abbia svolto la valutazione di conformità, redatto la documentazione tecnica, apposto la marcatura CE e designato un rappresentante autorizzato ove necessario.
- Non immettere sul mercato sistemi non conformi; informare fornitore e autorità in caso di rischio.
- Conservare la documentazione e assicurare che le condizioni di magazzino e trasporto non compromettano la conformità.
- Cooperare con le autorità e fornire su richiesta tutte le informazioni necessarie.

8.5 Pubbliche amministrazioni ed enti pubblici

La PA cumula il ruolo di deployer con obblighi aggiuntivi, sia europei sia nazionali.

- Valutazione d'impatto sui diritti fondamentali (FRIA) prima dell'uso di sistemi ad alto rischio, con obbligo di notifica all'autorità di vigilanza del mercato.
- Registrazione nella banca dati UE dell'uso dei sistemi ad alto rischio.
- Trasparenza rafforzata verso i cittadini: obbligo di rendere noto quando un contenuto o una comunicazione è generata da IA.
- Principi della legge 132/2025 in materia di uso dell'IA nell'attività amministrativa: la decisione resta imputabile al funzionario responsabile, con tracciabilità e conoscibilità del funzionamento del sistema.
- Regime transitorio: per i sistemi ad alto rischio immessi sul mercato prima delle date di applicazione, l'adeguamento è dovuto entro il 2 agosto 2030, salvo modifiche sostanziali.
- Coordinamento con la disciplina degli appalti: i requisiti di conformità all'AI Act sono destinati a diventare criteri di ammissione e di valutazione delle offerte.

8.6 Il presidio contrattuale: le clausole tipo europee e le linee guida per il procurement

Torniamo su un punto già emerso due volte, al § 3.2 a proposito di chi diventa fornitore senza accorgersene e al § 11.2 a proposito della responsabilità da prodotto. È il punto in cui questa guida diventa, molto concretamente, una questione di contratti.

Il regolamento distribuisce gli obblighi per ruolo, ma quasi nessuna impresa è in grado di adempiere da sola. Chi usa un sistema di terzi deve poterlo utilizzare secondo istruzioni che qualcun altro ha scritto, dimostrare caratteristiche che qualcun altro ha determinato, segnalare incidenti che qualcun altro rileva per primo. Se il contratto non prevede tutto questo, la conformità resta un'intenzione.

Le clausole contrattuali tipo della Commissione europea
La Commissione ha messo a disposizione clausole contrattuali tipo per l'acquisto di sistemi di intelligenza artificiale, in due versioni: una per i sistemi ad alto rischio, più stringente, e una per i sistemi che non lo sono. Sono nate per gli acquisti delle amministrazioni pubbliche, ma nulla ne impedisce l'uso in ambito privato, e anzi rappresentano la base negoziale più comoda che un'impresa possa portare al tavolo, perché sono neutre e riconoscibili da entrambe le parti.

Le clausole sono organizzate per aree tematiche e coprono, fra l'altro, la conformità del sistema, i ruoli e le responsabilità del fornitore e la governance dei dati. Due avvertenze sono però essenziali. La prima: l'adesione è volontaria, non sono un modello obbligatorio. La seconda, più importante nella pratica: le clausole si occupano esclusivamente di quanto discende dall'AI Act e non disciplinano proprietà intellettuale, corrispettivi, legge applicabile e responsabilità contrattuale generale. Chi le adotta pensando di avere un contratto completo si troverà scoperto proprio sui temi che generano il maggior numero di contenziosi.
Per le amministrazioni si aggiungono le linee guida di AgID sul procurement di intelligenza artificiale, allineate al quadro europeo e centrate su trasparenza, responsabilità e controllo umano sulle decisioni automatizzate.

Le clausole minime, per chiunque acquisti IA
Al di là dei modelli, questi sono i punti che in un contratto di fornitura non dovrebbero mancare.

- Qualificazione dei ruoli. Chi è fornitore e chi deployer rispetto a quel sistema, e che cosa succede se l'acquirente lo personalizza o lo presenta con il proprio marchio. È il modo per non scoprire a posteriori di aver assunto gli obblighi del produttore.
- Documentazione e istruzioni per l'uso. Consegna delle istruzioni, impegno a mantenerle aggiornate, e accesso alla documentazione tecnica necessaria per rispondere alle autorità.
- Dichiarazione di conformità e impegno di adeguamento. Oltre allo stato attuale, l'impegno ad adeguarsi entro le scadenze del 2 dicembre 2027 e del 2 agosto 2028, con conseguenze contrattuali in caso contrario.
- Trasparenza. Chi implementa la marcatura dei contenuti sintetici e l'avviso di interazione con un'IA, e con quali soluzioni tecniche.
- Uso dei dati. Finalità consentite, divieto di riutilizzo dei dati del cliente per l'addestramento salvo accordo espresso, localizzazione, catena dei subfornitori.
- Sicurezza e incidenti. Tempi e modalità di notifica, obbligo di cooperazione nelle segnalazioni alle autorità.
- Aggiornamenti. Impegno a fornire aggiornamenti, inclusi quelli di sicurezza, per tutta la durata del rapporto: è il presupposto per non trovarsi con un prodotto che diventa difettoso per omissione, come si è visto al § 11.2.
- Audit e verifiche. Diritto di verificare, direttamente o tramite terzi, quanto dichiarato.
- Ripartizione delle responsabilità e manleve, coordinate con il regime della responsabilità da prodotto e non solo con l'inadempimento contrattuale.
- Uscita. Portabilità dei dati e reversibilità del servizio, tema su cui il Data Act offre argomenti (§ 10.2).

Il momento giusto
Tutto questo si negozia prima della firma. Dopo, il potere contrattuale è quasi sempre evaporato: il sistema è in produzione, le persone sono formate, i processi ci girano intorno. Vale la pena guardare anche ai contratti già in essere in vista del rinnovo: è l'unica finestra in cui si può chiedere qualcosa senza pagarlo due volte.

9. Il livello italiano: la legge 132/2025 e i decreti attuativi

L'Italia è stato il primo Stato membro a dotarsi di una legge nazionale organica sull'intelligenza artificiale. La legge 23 settembre 2025, n. 132, in vigore dal 10 ottobre 2025, non duplica l'AI Act, in quanto ne presuppone l'applicazione e interviene sugli spazi lasciati agli Stati e su materie di competenza nazionale: lavoro, professioni, sanità, giustizia, diritto penale.

9.1 Gli obblighi che riguardano direttamente le imprese

Ambito	Obbligo	Riferimento
Lavoro	Il datore di lavoro che impiega sistemi di IA per la gestione del rapporto deve informare per iscritto il lavoratore e le rappresentanze sindacali. L'informativa va resa al momento della costituzione del rapporto e comunque prima dell'inizio dell'utilizzo.	Art. 11 L. 132/2025, che richiama l'art. 1-bis del D.Lgs. 152/1997
Professioni intellettuali	L'uso dell'IA è consentito come supporto strumentale; il professionista deve informare il cliente in modo chiaro e comprensibile sui sistemi utilizzati. La prestazione intellettuale resta prevalentemente umana.	Artt. 12-13 L. 132/2025
Sanità	L'IA è di supporto alla prevenzione, diagnosi e cura: la decisione resta al medico. Obbligo di informare il paziente sull'uso di sistemi di IA.	Artt. 7-8 L. 132/2025
Minori	Per l'accesso a tecnologie di IA da parte di minori di quattordici anni è richiesto il consenso di chi esercita la responsabilità genitoriale.	Art. 4 L. 132/2025
Governance	AgID è autorità di notifica degli organismi di valutazione della conformità; ACN è autorità di vigilanza del mercato, con poteri ispettivi e sanzionatori. Restano ferme le competenze del Garante privacy, di Banca d'Italia, CONSOB e IVASS.	Artt. 23-24 L. 132/2025 e schemi di decreto attuativo

9.2 IA e diritto d'autore: che cosa si può proteggere e che cosa no

Se la vostra azienda produce contenuti (testi, immagini, video, musica, codice, materiali di marketing), questa è probabilmente la parte della legge italiana che vi riguarda più da vicino. E il punto di partenza è controintuitivo: il rischio principale non è violare i diritti altrui, ma scoprire di non avere diritti propri.
L'opera resta umana
La legge 132/2025 è intervenuta sull'articolo 1 della legge sul diritto d'autore, la 633 del 1941. La nuova formulazione include espressamente le opere create con l'ausilio di strumenti di intelligenza artificiale,

ma a una condizione: che il risultato sia riconducibile all'attività intellettuale dell'autore. L'IA è uno strumento, non un autore.
La conseguenza pratica è netta. Un contenuto interamente generato da un sistema, senza un apporto creativo umano riconoscibile, non gode di protezione: nessuna esclusiva, nessun diritto di impedire ad altri di usarlo. Se un'agenzia consegna un'immagine prodotta con un prompt e nient'altro, quell'immagine resta materiale che chiunque può riutilizzare, e non un asset che l'azienda possiede.
Il punto delicato sta nella prova, più che nel principio. Chi rivendica la titolarità di un'opera realizzata con l'IA deve poter dimostrare l'apporto umano: bozze, versioni intermedie, scelte di impostazione, interventi di editing, direzione creativa documentata. È una questione di archivio, prima che di diritto.

L'addestramento e l'estrazione di testi e dati
Il secondo intervento riguarda il lato opposto: usare opere altrui per addestrare o alimentare un sistema. Il nuovo articolo 70-septies della legge 633/1941 chiarisce che la riproduzione e l'estrazione di opere e altri materiali attraverso modelli e sistemi di intelligenza artificiale, anche generativi, sono consentite nei limiti già previsti dagli articoli 70-ter e 70-quater, le eccezioni per l'estrazione di testi e dati introdotte con la direttiva europea sul copyright.
Quei limiti contengono un meccanismo che le imprese titolari di contenuti dovrebbero conoscere: al di fuori della ricerca scientifica, il titolare dei diritti può riservarsi espressamente l'utilizzo delle proprie opere per l'estrazione di testi e dati. Se la riserva è manifestata in modo appropriato (tipicamente, per i contenuti online, in forma leggibile automaticamente), l'eccezione non opera. Chi pubblica cataloghi, banche dati, archivi fotografici o contenuti editoriali ha quindi una scelta da fare, e non farla equivale a consentire.
Sul versante europeo la questione torna dall'altro capo: l'AI Act impone ai fornitori di modelli per finalità generali di adottare una politica di rispetto del diritto d'autore, incluse le riserve di estrazione, e di pubblicare una sintesi dei contenuti usati per l'addestramento. Le due discipline si tengono: l'una dà al titolare lo strumento per dire di no, l'altra obbliga chi addestra a rispettarlo e a rendere conto.

Tre cose da fare, in ordine di urgenza
Nei contratti con agenzie e creativi: inserire una dichiarazione sull'uso di strumenti di IA e una garanzia sull'apporto creativo umano, con l'obbligo di conservare i materiali che lo documentano. Senza questo, si acquista un contenuto senza sapere se si acquista anche un diritto.
Sugli asset identitari: marchi, loghi, personaggi e mascotte non andrebbero costruiti su output puramente generativi. Un marchio si tutela per altra via, ma l'elemento figurativo privo di protezione autoriale è più esposto all'imitazione.
Sui contenuti che pubblicate: valutare se manifestare la riserva sull'estrazione di testi e dati, in forma leggibile automaticamente. È una decisione di strategia, non un adempimento, ma è una decisione, e il silenzio è una risposta.

9.3 I profili penali

La legge ha introdotto nel Codice penale una nuova fattispecie che punisce con la reclusione da uno a cinque anni chi cagiona un danno ingiusto cedendo, pubblicando o comunque diffondendo, senza il consenso della persona interessata, immagini, video o voci falsificati o alterati mediante sistemi di intelligenza artificiale e idonei a indurre in inganno sulla loro autenticità. Non basta la diffusione, perché occorre un danno ingiusto concreto: alla reputazione, alla dignità, all'identità personale, alla vita privata.
È stata inoltre introdotta un'aggravante comune per i reati commessi mediante l'impiego di sistemi di intelligenza artificiale, quando ciò abbia ostacolato la difesa o aggravato le conseguenze del fatto, e sono state inasprite alcune fattispecie esistenti: dalla truffa alla sostituzione di persona, dalla manipolazione del mercato all'aggiotaggio.

Perché interessa anche le imprese
Questi reati non riguardano soltanto i comportamenti individuali. Una campagna di marketing che utilizzi la voce o il volto sintetico di una persona reale senza consenso, un contenuto generato per una comunicazione aziendale, l'uso di avatar realistici in ambito commerciale: sono situazioni che possono integrare la fattispecie e che richiedono un presidio autorizzativo interno.
Per le società dotate di modello organizzativo ex D.Lgs. 231/2001, è opportuno verificare se e in che misura i reati aggravati dall'uso dell'IA rientrino nel catalogo dei reati presupposto, e aggiornare di conseguenza la mappatura dei rischi e le procedure.

9.4 Lo stato dei decreti attuativi e il parere del Garante

Il Consiglio dei Ministri del 10 giugno 2026 ha approvato in esame preliminare due schemi di decreto legislativo. Il primo disciplina i poteri delle autorità nazionali, la vigilanza e le sanzioni, gli spazi di sperimentazione, la formazione e le disposizioni in materia di lavoro.
Il secondo regola l'impiego dell'IA nelle attività di polizia e interviene sulla responsabilità civile e penale. L'iter parlamentare consultivo è in corso; il termine per l'esercizio della delega scade il 10 ottobre 2026. Nel corso di quell'iter il Garante per la protezione dei dati personali ha reso il proprio parere sugli schemi, chiedendo tutele più solide sul trattamento dei dati e, in particolare, sull'uso delle tecnologie biometriche; il Presidente dell'Autorità è stato inoltre audito in Parlamento. Non si tratta di un passaggio formale: i rilievi riguardano proprio i punti di contatto fra la disciplina dell'IA e quella dei dati personali, cioè l'area in cui le imprese incontrano più spesso vincoli operativi.

Che cosa se ne ricava, per chi deve decidere oggi.
Fino all'adozione definitiva il quadro nazionale di dettaglio (procedimento sanzionatorio, riparto operativo delle competenze fra le autorità, regole di funzionamento dello spazio di sperimentazione) non è completo, e il testo che circola può ancora cambiare proprio nelle parti oggetto dei rilievi. Questo non sospende nulla: gli obblighi europei sono direttamente applicabili e le autorità hanno già i loro poteri. Ma sconsiglia due cose. La prima è costruire procedure interne sul testo di uno schema non ancora definitivo. La seconda è l'opposto, ed è l'errore più comune: aspettare il decreto per cominciare, quando ciò che il decreto disciplina è il come si sanziona, non il se si è obbligati.

10. Le altre normative che si intrecciano con l'AI Act

L'AI Act non è un'isola. Nella pratica, i progetti di intelligenza artificiale si fermano quasi sempre per ragioni che con l'AI Act non hanno nulla a che vedere: una base giuridica che manca, un contratto cloud che non consente di portare via i dati, un fornitore che non supera la verifica di sicurezza. Questo capitolo non tratta quelle discipline (servirebbe un documento per ciascuna) ma le colloca, in modo che sappiate quando chiamare in causa qualcun altro oltre al referente per l'IA.

10.1 GDPR: due discipline, due autorità, due procedimenti

È la sovrapposizione più frequente e la più fraintesa, perché le due normative non si escludono e non si assorbono: proteggono cose diverse. L'AI Act tutela salute, sicurezza e diritti fondamentali attraverso la logica della sicurezza dei prodotti, e guarda al sistema. Il GDPR tutela le persone rispetto al trattamento dei loro dati, e guarda al trattamento. Quasi ogni sistema di IA aziendale ricade in entrambe.

In concreto, per un sistema che tratta dati personali restano da verificare: la base giuridica del trattamento, sia per l'uso sia, punto spesso trascurato, per l'eventuale addestramento; l'informativa agli interessati; la valutazione d'impatto sulla protezione dei dati, che nei casi più comuni di IA applicata alle persone è dovuta; e l'articolo 22, che riconosce all'interessato il diritto di non essere sottoposto a decisioni interamente automatizzate che producano effetti giuridici o significativi, con diritto all'intervento umano, alla spiegazione e alla contestazione.
Le autorità sono diverse: la vigilanza del mercato sull'IA spetta all'ACN, la protezione dei dati al Garante. Gli stessi fatti possono quindi dare luogo a due procedimenti autonomi, davanti a due autorità, con due sanzioni. Il § 11.3 mostra che, ad oggi, è il secondo canale ad aver prodotto i provvedimenti concreti.
C'è però anche un'economia di scala da sfruttare. La valutazione d'impatto sulla protezione dei dati e il sistema di gestione del rischio richiesto dall'AI Act sono documenti distinti, con finalità diverse, ma si nutrono degli stessi materiali: la mappatura del sistema, la descrizione dei dati, l'analisi dei rischi per le persone. Farli separatamente, a distanza di mesi e con fornitori diversi, è il modo più costoso di arrivare allo stesso risultato.
Un'avvertenza sul futuro: il pacchetto di semplificazione sui dati, ancora in discussione, potrebbe modificare proprio i punti di contatto fra le due discipline, a partire dal legittimo interesse come base per l'addestramento dei sistemi. Se ne è detto al § 7.2.

10.2 Data Act, NIS2, DORA e il perimetro della cybersicurezza

Data Act, Regolamento (UE) 2023/2854. Applicabile dal 12 settembre 2025, con alcune previsioni a decorrenza differita: l'obbligo di progettare i nuovi dispositivi connessi in modo da consentire l'accesso ai dati riguarda quelli immessi sul mercato dopo il 12 settembre 2026, e la disciplina sulle clausole contrattuali abusive va a regime nel 2027. Riguarda l'accesso ai dati generati da prodotti connessi e servizi correlati, la loro condivisione e il passaggio da un fornitore cloud a un altro. Interessa l'intelligenza artificiale da due lati: chi addestra modelli su dati industriali o di prodotti connessi deve sapere a chi quei dati spettano, e chi ospita i propri sistemi in cloud dovrebbe verificare le clausole di uscita prima di costruirci sopra un progetto.
NIS2, direttiva (UE) 2022/2555, recepita in Italia con il D.Lgs. 138/2024. Individua soggetti essenziali e importanti in una serie di settori e impone misure di sicurezza, obblighi di registrazione presso la piattaforma dell'ACN e notifica degli incidenti secondo tempi stretti: pre-notifica entro 24 ore, notifica entro 72 ore, relazione finale entro un mese. Il calendario italiano prosegue nel 2026 con l'attuazione delle misure di sicurezza di base. Se rientrate nel perimetro, i vostri sistemi di IA sono sistemi informatici come gli altri, e la responsabilità degli organi di amministrazione sulla sicurezza li comprende.
DORA, Regolamento (UE) 2022/2554. Applicabile dal 17 gennaio 2025 agli enti finanziari e ai fornitori di servizi ICT considerati critici. Chi fornisce soluzioni di IA a banche, assicurazioni o intermediari finisce nel perimetro del rischio informatico da terze parti, con requisiti contrattuali stringenti su continuità, audit e strategie di uscita: un fornitore che non li accetta è, di fatto, un fornitore che quel cliente non può usare.

Il filo comune
L'articolo 15 dell'AI Act chiede ai sistemi ad alto rischio accuratezza, robustezza e cybersicurezza. Sono, in larga parte, le stesse misure che un'impresa già implementa per NIS2 o per DORA. La raccomandazione pratica è quindi di non costruire un secondo impianto parallelo: conviene estendere il perimetro di quello esistente ai sistemi di IA, riutilizzando politiche, procedure di gestione degli incidenti e valutazioni sui fornitori.

10.3 Le regole settoriali: finanza, sanità, lavoro

Finanza e assicurazioni. La valutazione del merito creditizio delle persone fisiche e la determinazione dei prezzi nelle assicurazioni vita e salute rientrano fra i sistemi ad alto rischio dell'Allegato III: gli obblighi arriveranno il 2 dicembre 2027. Nel frattempo restano ferme le competenze di Banca d'Italia, CONSOB e IVASS, che sui modelli chiedono già oggi governance, documentazione e controlli interni. Per gli operatori vigilati, la conformità all'AI Act si innesta su un impianto che in buona parte esiste già.
Sanità e dispositivi medici. Un software di IA che ha una finalità medica è un dispositivo medico ai sensi del Regolamento (UE) 2017/745 e segue quella disciplina: marcatura CE, organismo notificato, sorveglianza post-commercializzazione. L'AI Act si aggiunge, e per i sistemi dell'Allegato I i suoi obblighi arriveranno il 2 agosto 2028. Le due valutazioni di conformità sono destinate a integrarsi, non a sommarsi meccanicamente.
Lavoro. È il settore con il maggior numero di norme concorrenti, ed è anche quello dove le imprese sbagliano più spesso. Oltre all'informativa prevista dalla legge 132/2025 di cui si è detto al § 9.1, va considerato l'articolo 4 dello Statuto dei lavoratori: gli strumenti da cui deriva anche solo indirettamente una possibilità di controllo a distanza dell'attività richiedono un accordo sindacale o un'autorizzazione amministrativa. Un sistema di IA che misura produttività, tempi o qualità del lavoro ricade tipicamente in questa previsione. Si aggiungono il divieto assoluto di riconoscimento delle emozioni sul luogo di lavoro e le indicazioni del Garante di cui al § 11.3.

Come usare questa mappa
Prima di avviare un progetto di IA, tre domande fanno emergere quasi tutte le sovrapposizioni. Il sistema tratta dati personali? Se sì, il GDPR viaggia in parallelo per tutta la durata del progetto. La mia impresa, o il mio cliente, rientra in un perimetro regolato (NIS2, DORA, dispositivi medici, vigilanza finanziaria)? Se sì, quel regolatore ha voce in capitolo prima e più dell'autorità sull'IA. Il sistema incide sui lavoratori? Se sì, servono relazioni sindacali oltre che adempimenti.

11. Le conseguenze: sanzioni, responsabilità e rischi

11.1 Le sanzioni amministrative dell'AI Act

Il regolamento fissa i massimali; gli Stati membri disciplinano il procedimento. Il criterio è quello, familiare a chi conosce il GDPR, dell'importo fisso o della percentuale sul fatturato mondiale annuo dell'esercizio precedente, applicando il valore più elevato.

Violazione	Massimale	Riferimento
Pratiche di IA vietate (art. 5)	Fino a 35 milioni di euro oppure fino al 7% del fatturato mondiale annuo totale, se superiore	Art. 99, par. 3
Inosservanza degli obblighi di fornitori, deployer, importatori, distributori e organismi notificati (compresi gli obblighi di trasparenza dell'art. 50)	Fino a 15 milioni di euro oppure fino al 3% del fatturato mondiale annuo totale, se superiore	Art. 99, par. 4

Violazione	Massimale	Riferimento
Comunicazione di informazioni inesatte, incomplete o fuorvianti a organismi notificati o autorità nazionali	Fino a 7,5 milioni di euro oppure fino all'1% del fatturato mondiale annuo totale, se superiore	Art. 99, par. 5
Inosservanza degli obblighi da parte dei fornitori di modelli GPAI (ammende irrogate dalla Commissione)	Fino a 15 milioni di euro oppure fino al 3% del fatturato mondiale annuo totale, se superiore	Art. 101 (applicabile dal 2 agosto 2026)
PMI e start-up	Si applica il valore inferiore fra l'importo fisso e la percentuale. Per le piccole imprese a media capitalizzazione va considerata la sostenibilità economica della sanzione.	Art. 99, par. 6; Reg. (UE) 2026/1744

Nel determinare l'importo, le autorità considerano la natura e la gravità della violazione, la sua durata, il numero di persone interessate, il carattere doloso o colposo, le misure adottate per attenuare il danno, la cooperazione prestata, le eventuali violazioni precedenti e la dimensione dell'operatore. Un programma di conformità documentato incide direttamente e concretamente sulla quantificazione.

11.2 La nuova responsabilità da prodotto difettoso: la scadenza del 9 dicembre 2026

Fin qui abbiamo parlato di sanzioni, cioè del rapporto fra l'impresa e l'autorità. Ma il rischio economicamente più rilevante, per chi sviluppa o incorpora intelligenza artificiale nei propri prodotti, viene da un'altra direzione: le cause civili di chi subisce un danno. Ed è proprio qui che sta la scadenza più vicina dopo il 2 agosto.
La direttiva (UE) 2024/2853 sostituisce la disciplina europea sulla responsabilità per danno da prodotti difettosi, ferma al 1985. Gli Stati membri devono recepirla entro il 9 dicembre 2026 e le nuove regole si applicano ai prodotti immessi sul mercato a partire da quella data. In Italia il recepimento è delegato al Governo dalla legge di delegazione europea 2025.

Il software è un prodotto
È il cambiamento di fondo. La direttiva del 1985 parlava di beni mobili, e per quarant'anni si è discusso se un programma per computer vi rientrasse. La nuova direttiva chiude la questione: sono prodotti i sistemi operativi, i firmware, le applicazioni, i programmi per computer e i sistemi di intelligenza artificiale, indipendentemente dal modo in cui sono distribuiti, cioè installati in locale, erogati in cloud, venduti come servizio o incorporati in un dispositivo fisico.
Per un'impresa che vende software con funzioni di IA, la conseguenza è netta: non risponde più soltanto per inadempimento contrattuale verso il proprio cliente, ma risponde del danno verso chiunque, anche verso chi non ha alcun rapporto con lei.

Che cosa deve provare chi agisce in giudizio
Il regime è di responsabilità oggettiva: il danneggiato non deve dimostrare che il produttore è stato negligente, ma soltanto il difetto, il danno e il nesso fra i due. La direttiva gli rende poi questa prova più agevole in due modi, pensati proprio per i casi in cui la tecnologia è opaca. Il giudice può ordinare al produttore di esibire gli elementi di prova in suo possesso; e quando la complessità tecnica o scientifica rende la prova eccessivamente difficile, può operare una presunzione sul difetto o sul nesso causale.

Chi conosce il funzionamento dei sistemi di apprendimento automatico capisce subito la portata del punto: la difficoltà di ricostruire perché un modello abbia prodotto un certo output cambia di segno, e da ostacolo per chi agisce diventa problema per chi si difende. La documentazione tecnica, i log e la tracciabilità richiesti dall'AI Act diventano allora anche il materiale con cui l'impresa dimostra di non avere colpa.

La responsabilità non si esaurisce con la vendita

È il secondo punto che tocca da vicino il software. Finché il produttore mantiene la capacità di fornire aggiornamenti o migliorie, direttamente o tramite terzi, il prodotto resta nella sua sfera di controllo. Un aggiornamento che introduce un difetto, o l'omissione di un aggiornamento di sicurezza necessario, possono rendere difettoso un prodotto che al momento dell'immissione sul mercato era perfettamente conforme.

Per i sistemi di IA, che apprendono e vengono ricalibrati nel tempo, questo significa che la conformità va mantenuta, non conseguita una volta sola.

Il parallelo con l'articolo 25 dell'AI Act

Chi modifica sostanzialmente un prodotto già immesso sul mercato risponde come se ne fosse il produttore. È la stessa logica che abbiamo incontrato al § 3.2 a proposito dell'AI Act: personalizzare in modo sostanziale un sistema di terzi sposta le responsabilità su di sé. Due discipline diverse, costruite sullo stesso principio, e questo rende il presidio contrattuale con i fornitori, di cui parliamo nel capitolo 8, ancora più importante.

11.3 L'enforcement reale oggi: i provvedimenti del Garante privacy

C'è un equivoco diffuso, ed è utile scioglierlo prima di chiudere il capitolo. Le sanzioni dell'AI Act sono diventate pienamente azionabili il 2 agosto 2026 e i primi procedimenti richiederanno tempo. Questo non significa però che chi usa l'intelligenza artificiale sia rimasto finora al riparo: significa che il canale sanzionatorio effettivamente attivo è stato un altro, il GDPR. I provvedimenti già adottati dicono molto su dove le autorità hanno guardato finora.

Intelligenza artificiale e luoghi di lavoro (provvedimento del 14 maggio 2026). Il Garante è intervenuto sull'uso di sistemi di IA in ambito lavorativo, con particolare attenzione agli strumenti che analizzano aspetti emotivi o psicologici dei lavoratori. Nel caso concreto non ha accertato violazioni, ma ha fissato un'indicazione di portata generale: il datore di lavoro non deve venire a conoscenza, neppure indirettamente, di informazioni relative alla sfera emotiva o psicologica dei dipendenti. È un principio che si somma al divieto assoluto di riconoscimento delle emozioni sul luogo di lavoro previsto dall'AI Act: due discipline diverse che, sullo stesso comportamento, arrivano alla stessa conclusione. Per un'impresa che stia valutando strumenti di analisi del clima aziendale, dell'engagement o della produttività individuale, è il provvedimento da leggere prima di firmare il contratto.

Character.AI (provvedimento del 3 luglio 2026, sanzione di 158.000 euro). Il Garante ha sanzionato la società statunitense che gestisce un servizio di IA generativa con cui gli utenti, anche minorenni, interagiscono con personaggi virtuali. Le contestazioni riguardano le garanzie a tutela dei minori e le procedure di verifica dell'età, la tardiva predisposizione della valutazione d'impatto sulla protezione dei dati e la tardiva designazione del rappresentante nell'Unione.

Vale la pena soffermarsi su quest'ultimo punto, perché è il più istruttivo. La sanzione ha colpito adempimenti organizzativi e documentali, non il funzionamento del modello: una valutazione d'impatto fatta tardi, un rappresentante nominato tardi. Sono esattamente le cose che qualsiasi impresa può

sbagliare, e che non richiedono competenze tecniche per essere messe a posto: solo di essere fatte prima, e non dopo.
OpenAI (dicembre 2024, sanzione di 15 milioni di euro e campagna informativa di sei mesi). Il precedente più noto, chiuso con una sanzione di importo assai superiore e con una misura atipica: l'obbligo di realizzare una campagna di informazione rivolta al pubblico.

Che cosa se ne ricava
Primo: gli stessi fatti possono essere esaminati da due autorità diverse, con due procedimenti e due sanzioni autonome. Un'impresa che ragiona soltanto sull'AI Act sta guardando metà del quadro: è il tema del § 10.1, nel capitolo sulle normative connesse.
Secondo: ciò che viene contestato, nella maggior parte dei casi, non è la tecnologia ma la mancanza di documentazione e di procedure. Valutazioni d'impatto non fatte o fatte in ritardo, informative incomplete, ruoli non designati. È la conferma pratica del principio di accountability che percorre tutto questo documento: essere conformi non basta, occorre poterlo dimostrare, e averlo fatto per tempo.

11.4 Le altre conseguenze non sanzionatorie, spesso più gravi

- Misure correttive e ritiro dal mercato. Le autorità di vigilanza possono imporre di conformare il sistema, ritirarlo o richiamarlo. Per un prodotto software distribuito, il costo operativo e reputazionale supera di regola quello della sanzione.
- Responsabilità contrattuale ed extracontrattuale. Al di fuori del danno da prodotto (di cui si è detto al § 11.2), restano applicabili le regole generali: l'inadempimento verso il cliente e l'illecito civile verso i terzi. Le vittime di decisioni automatizzate discriminatorie possono agire per il risarcimento indipendentemente da qualsiasi procedimento sanzionatorio.
- Sanzioni GDPR cumulabili. La violazione dell'AI Act che comporta anche un trattamento illecito di dati personali espone a un secondo procedimento, davanti a un'autorità diversa, con massimali propri.
- Esclusione da gare e contratti. La conformità è già oggi requisito nei capitolati pubblici e clausola standard nei contratti B2B, con diritti di audit e penali.
- Nullità o inefficacia di clausole e atti. Una decisione automatizzata assunta in violazione degli obblighi informativi può essere contestata nel merito, ad esempio in materia di lavoro.
- Rischio penale personale per gli esponenti aziendali, nelle ipotesi previste dalla legge 132/2025.
- Danno reputazionale. In un contesto in cui la fiducia è il principale ostacolo all'adozione dell'IA, un provvedimento pubblico ha un impatto commerciale difficile da recuperare.

12. Che cosa fare adesso: una roadmap praticabile

Le attività che seguono sono ordinate per urgenza e non per complessità, e i primi trenta giorni richiedono soprattutto tempo di persone, non investimenti. Dove la roadmap dice che cosa fare, il capitolo 13 risponde a come farlo nelle situazioni che si presentano davvero.

12.1 Entro 30 giorni: mettere a fuoco

- Costruire l'inventario dei sistemi di IA. Un elenco di tutti gli strumenti in uso o in sviluppo, compresi quelli adottati autonomamente dalle funzioni aziendali senza passare dall'IT (la cosiddetta shadow AI, che nella pratica è la fonte principale di sorprese). Per ciascuno: fornitore, finalità, dati trattati, funzione utilizzatrice, referente interno.
- Qualificare il ruolo per ciascun sistema: fornitore, deployer, importatore, distributore. Verificare in particolare i casi di rebranding o personalizzazione che potrebbero far scattare l'articolo 25.
- Verificare l'assenza di pratiche vietate. È un controllo rapido con conseguenze gravissime se trascurato: il massimale è il più alto previsto dal regolamento.
- Fare l'audit della trasparenza. Ogni punto di contatto con clienti, utenti o cittadini: chatbot, assistenti vocali, contenuti generati per il sito o i social, comunicazioni automatizzate. Verificare che sia dichiarato ciò che va dichiarato.
- Verificare che l'informativa ai lavoratori e alle rappresentanze sindacali sia stata resa e sia aggiornata.

12.2 Entro 90 giorni: presidiare

- Adottare una policy aziendale sull'uso dell'IA: strumenti autorizzati, usi vietati, gestione dei dati riservati e personali, obbligo di revisione umana degli output, tracciabilità delle decisioni.
- Definire ruoli e responsabilità: chi autorizza l'adozione di un nuovo strumento, chi valuta il rischio, chi presidia la relazione con i fornitori. Coinvolgere IT, HR, legale, DPO e le funzioni di business.
- Erogare la formazione e conservarne evidenza: destinatari, contenuti, date, materiali. È l'adempimento con il miglior rapporto fra costo e valore difensivo.
- Rivedere la contrattualistica con i fornitori di tecnologia: dichiarazioni di conformità, impegni di aggiornamento, documentazione tecnica, diritti di audit, ripartizione delle responsabilità, obblighi di notifica degli incidenti.
- Aggiornare le informative privacy e verificare la necessità di valutazioni d'impatto sulla protezione dei dati.

12.3 Entro 12 mesi: costruire

- Classificare i sistemi rispetto agli Allegati I e III per individuare quelli che diventeranno ad alto rischio, e costruire il piano di adeguamento verso il 2 dicembre 2027.
- Impostare un sistema di gestione del rischio dell'IA, eventualmente ancorandolo alla norma ISO/IEC 42001, che offre una struttura riconosciuta e certificabile.
- Predisporre la documentazione tecnica per i sistemi di cui siete fornitori.
- Monitorare le norme armonizzate CEN-CENELEC e gli aggiornamenti delle linee guida della Commissione.
- Valutare l'adesione ai codici di buone pratiche e, per progetti innovativi, l'accesso allo spazio di sperimentazione nazionale

Il principio che tiene insieme tutto
L'AI Act è una normativa di accountability: non chiede soltanto di essere conformi, chiede di essere in grado di dimostrarlo. Una decisione ragionata e messa per iscritto (anche quella di non fare qualcosa, con le ragioni che la sostengono) vale, davanti a un'autorità, incomparabilmente più di una conformità sostanziale non documentata.

13. FAQ sui casi concreti

Le domande che seguono nascono da situazioni reali, ogni risposta dichiara le fonti sulle quali si appoggia, poiché in questa materia il confine fra ciò che è scritto e ciò che è opinabile è molto labile.

Tre sono i gradi di affidabilità delle fonti e ricalcano la gerarchia del capitolo 2.

Grado	Che cosa significa
Testo normativo	La risposta sta in un articolo del regolamento o di una legge, citato per numero. È vincolante.
Orientamento	La risposta sta in linee guida della Commissione, in un codice di buone pratiche o in un provvedimento di un'autorità. Non vincola in senso stretto, ma è il metro con cui sarete valutati.
Aperta	Esistono solo letture dottrinali o fonti secondarie. La risposta dice che cosa scioglierebbe il dubbio e dove guardare.

Una stessa domanda può comprendere due gradi differenti di affidabilità, ed è il caso più frequente: quando questo accade viene segnalato, in questo modo una parte solida non legittima necessariamente quella fragile che le sta accanto.

I quesiti sono numerati da D1 a Dx

D1. I contenuti già online prima del 2 agosto 2026 vanno etichettati a ritroso?

No. La ragione non sta nel silenzio della norma, ma in una scelta che il legislatore ha compiuto altrove: il Regolamento (UE) 2026/1744 ha introdotto nell'AI Act l'articolo 111, paragrafo 4, che impone ai fornitori di sistemi generativi già immessi sul mercato prima del 2 agosto 2026 di conformarsi entro il 2 dicembre 2026 alle regole di marcatura dell'articolo 50, paragrafo 2. Un regime transitorio, quindi, è stato previsto; riguarda però i sistemi e la loro capacità di marcare ciò che producono, non i contenuti che sono già stati pubblicati.
Per l'impresa la conseguenza pratica è che gli archivi non vanno ripercorsi. Chi negli anni scorsi ha pubblicato immagini, video o testi prodotti con l'IA non deve tornare indietro a marcarli, e questo vale sia per il sito sia per i profili social.
Fondamento: articolo 111, paragrafo 4, dell'AI Act, come introdotto dal Reg. (UE) 2026/1744; articolo 50, paragrafo 2. **Grado:** testo normativo
Resta però un caso che in redazione capita spesso, ed è quello del testo generato prima del 2 agosto e pubblicato dopo. Secondo una fonte secondaria va etichettato, e il ragionamento tiene, perché il fatto che l'articolo 50 disciplina è la messa a disposizione del contenuto e non il momento in cui è stato generato; il riscontro sugli orientamenti della Commissione però manca. Nel dubbio consigliamo di

etichettare: costa una riga, e il rischio dall'altra parte è una sanzione fino a 15 milioni di euro o al 3% del fatturato mondiale (§ 11.1).
Fondamento: nessuna fonte primaria; una sola fonte secondaria, da riscontrare sugli orientamenti del 20 luglio 2026. **Grado:** aperta

D2. Nelle campagne a pagamento il flag che la piattaforma mette a disposizione basta a mettersi in regola?

Aiuta, ed è la strada giusta, ma non chiude la questione, perché non sposta la responsabilità di un millimetro. L'obbligo dell'articolo 50, paragrafo 4, grava sul deployer, termine che il regolamento non traduce e che in italiano rendiamo con utilizzatore: l'articolo 3, numero 4, lo definisce come chi utilizza un sistema di IA sotto la propria autorità nell'ambito di un'attività professionale (§ 3.1).
In una campagna pubblicitaria l'utilizzatore è l'impresa che decide di diffondere quel contenuto e lo presenta con il proprio nome, non la piattaforma che si limita a ospitarlo. L'agenzia che carica materialmente l'annuncio agisce per conto vostro e non vi sostituisce; può però diventare utilizzatore a sua volta, se genera il contenuto con strumenti propri e sotto la propria autorità, ed è una delle ragioni per cui il § 8.6 insiste tanto sui contratti. L'informazione, in ogni caso, va resa in modo chiaro e distinguibile al più tardi al momento della prima esposizione: il flag è un mezzo con cui adempiete voi, non un adempimento che la piattaforma compie al posto vostro.
Fondamento: articolo 3, numero 4, e articolo 50, paragrafi 4 e 5, dell'AI Act · **Grado:** testo normativo

Gli orientamenti della Commissione del 20 luglio 2026 lo dicono in modo che vale la pena conoscere: fra i mezzi con cui il deployer assicura la trasparenza indicano le impostazioni di interfaccia e le condizioni contrattuali con i partner di distribuzione. Il flag rientra quindi a pieno titolo fra gli strumenti ammessi, ma è nominato come uno dei modi in cui garantite un risultato, e il risultato è che l'etichetta resti effettivamente visibile a chi incontra il contenuto per la prima volta. Gli stessi orientamenti precisano che chi si limita a ospitare o distribuire contenuti altrui non è utilizzatore e non ha obblighi propri di trasparenza: la piattaforma vi offre un interruttore, non una copertura.
Fondamento: orientamenti della Commissione sugli obblighi di trasparenza, 20 luglio 2026 · **Grado:** orientamento
Le accortezze che ne discendono sono quattro.

- Verificare la resa. Il flag va acceso, ma poi va guardato: la stessa creatività compare su posizionamenti diversi, e l'etichetta non viene resa allo stesso modo dappertutto. Il controllo si fa sull'annuncio pubblicato, non sul pannello di configurazione.
- Portare l'obbligo nei contratti. È il mezzo che gli orientamenti nominano accanto alle impostazioni di interfaccia, e riguarda agenzie, concessionarie, creator e chiunque pubblichi per conto vostro. Il § 8.6 tratta la contrattualistica per esteso.
- Conservare l'evidenza. Uno scatto dell'impostazione e uno dell'annuncio in pagina, archiviati con la campagna. Vale qui il principio che percorre tutto il documento: essere conformi non basta, occorre poterlo dimostrare (§ 11.3).
- Marcare la creatività quando il contenuto viaggia. Un'immagine o un video destinati a essere riusati fuori dalla piattaforma perdono il flag insieme al posizionamento, mentre una marcatura dentro il file resta.

Un'ultima avvertenza, che è la fonte di equivoco più comune. Diverse piattaforme espongono da anni una dichiarazione sull'uso di contenuti creati o alterati digitalmente, pensata per gli annunci di natura politica o sociale: è una regola della piattaforma, con un perimetro suo, e averla compilata non significa avere assolto l'articolo 50. Sono due adempimenti distinti che a volte condividono la stessa casella.
Fondamento: ricostruzione dalle politiche delle piattaforme, non dall'AI Act · **Grado:** aperta

D3. Sui contenuti organici, dove il flag spesso non c'è, valgono le stesse regole delle campagne?

La regola è la stessa, cambiano i mezzi. L'articolo 50 non distingue fra contenuto a pagamento e contenuto organico: a far scattare l'obbligo è la natura di ciò che pubblicate, cioè un deepfake oppure un testo diffuso per informare il pubblico su questioni di interesse pubblico, non il modo in cui il post raggiunge le persone. Sul piano giuridico un reel organico e un annuncio sponsorizzato stanno quindi sullo stesso piano, e l'assenza dell'interruttore non attenua nulla: sposta solo su di voi il lavoro che altrove fa l'interfaccia.

Fondamento: articolo 50, paragrafi 4 e 5, dell'AI Act · **Grado:** testo normativo

Prima di tutto il resto conviene però restringere il campo, perché l'errore più diffuso va nella direzione opposta e consiste nel dichiarare tutto. La maggior parte dei post aziendali resta fuori dall'articolo 50, e la ragione sta in due definizioni precise che vale la pena leggere prima di scrivere una policy.

La prima è quella di deep fake, all'articolo 3, numero 60: immagini o contenuti audio o video generati o manipolati dall'IA «che assomigliano a persone, oggetti, luoghi o altre entità o eventi esistenti e che apparirebbero falsamente autentici o veritieri a una persona». Servono quindi due requisiti insieme, la somiglianza con qualcosa di esistente e l'apparenza di autenticità: un drago, un pianeta immaginario o un'illustrazione dichiaratamente stilizzata non soddisfano né l'uno né l'altra.

La seconda è il perimetro dei testi, al paragrafo 4, secondo comma: riguarda i testi «pubblicati allo scopo di informare il pubblico su questioni di interesse pubblico», e non ogni testo che pubblicate. Un post che presenta un prodotto o racconta un'assunzione non informa su una questione collettiva, e resta fuori a prescindere da come è stato scritto.

Che cosa pubblicate	Obbligo	Perché
Video in cui la voce o il volto di una persona reale (il fondatore, un dipendente, un testimonial) è ricostruito o doppiato con l'IA	Sì	Persona esistente, apparenza autentica: è la definizione di deep fake
Fotografia realistica di un luogo esistente modificata per mostrare qualcosa che non c'è, per esempio la vostra sede con una linea produttiva mai installata	Sì	Luogo esistente presentato come autentico
Testo generato dall'IA e pubblicato sul blog aziendale per spiegare una novità normativa, sanitaria o ambientale, senza che nessuno lo abbia riletto nel merito	Sì	Testo di interesse pubblico, e l'esenzione per revisione umana non opera
Assistente conversazionale sul sito, nei messaggi diretti o nei commenti	Sì	Ricade nel paragrafo 1, quello sull'interazione, e vale anche se non genera contenuti
Fotografia di un prodotto reale con ritocco, scontorno o correzione di luce fatti con strumenti di IA	No	Nessuna apparenza falsamente autentica: resta la cosa che è
Illustrazione, icona, infografica o immagine dichiaratamente stilizzata, anche se generata per intero	No	Non assomiglia a entità esistenti e non appare autentica
Copy promozionale scritto con l'assistenza dell'IA e riletto da voi	No	Non è un testo di interesse pubblico: il perimetro non si apre nemmeno

Che cosa pubblicate	Obbligo	Perché
Traduzione automatica di un vostro testo già pubblicato	No	Nessun contenuto nuovo generato o manipolato ai fini dell'articolo 50
Contenuto manifestamente artistico, satirico o di finzione	Attenuato	L'obbligo esiste ma si assolve senza ostacolare la fruizione, per esempio nei titoli di coda (§ 6.1)
Persona sintetica che non esiste ma appare reale, usata come testimonial	Incerto	Vedi sotto: la definizione richiede la somiglianza con persone esistenti

Fondamento: articolo 3, numero 60, e articolo 50, paragrafi 1 e 4, dell'AI Act · **Grado:** testo normativo
Due righe della tabella meritano una spiegazione in più, perché è lì che si sbaglia.
Il testo riletto. L'esenzione del secondo comma non si accontenta di una passata veloce: gli orientamenti chiedono che la revisione sia svolta da persone con conoscenze adeguate alla materia, che riguardi il contenuto e comprenda almeno la verifica dell'accuratezza delle informazioni. Una correzione grammaticale non basta, una revisione fatta da un altro sistema di IA nemmeno, e un successivo intervento sostanziale dell'IA fa decadere l'esenzione già maturata. Chi rilegge, inoltre, deve assumersi la responsabilità editoriale della pubblicazione, il che significa che qualcuno con un nome e un cognome ci mette la faccia.
La persona sintetica. Un volto generato che non corrisponde a nessuno ma sembra reale è il caso di confine più frequente nel marketing, e la definizione dell'articolo 3 non lo risolve, perché richiede la somiglianza con persone esistenti. Nessuna fonte consultata prende posizione. Noi suggeriamo di dichiarare comunque, per due ragioni pratiche: la somiglianza casuale con una persona reale è un rischio concreto quando il volto è fotorealistico, e la dichiarazione costa una riga mentre la contestazione costa un procedimento.
Fondamento: orientamenti della Commissione del 20 luglio 2026 per la revisione umana · Grado: orientamento. Nessuna fonte sul testimonial sintetico · **Grado:** aperta
Dentro quel perimetro, quattro cose cambiano rispetto alla campagna.

- La dichiarazione la scrivete voi. Va in apertura della didascalia, non in fondo dopo gli hashtag, e deve essere percepibile senza strumenti tecnici: gli orientamenti della Commissione escludono che possa essere relegata in nota, e i metadati da soli non bastano.
- Il segno va dentro la creatività. Un post organico viene ricondiviso e incorporato molto più di un annuncio, e la didascalia si perde per strada mentre una marcatura visibile nell'immagine o nel video resta.
- Serve una regola, non un giudizio caso per caso. L'organico è ad alta frequenza e passa per molte mani, quindi la valutazione va scritta una volta nella policy sull'uso dell'IA (§ 12.2) e non lasciata a chi pubblica alle otto di sera.
- Le risposte automatiche stanno altrove. Un assistente che risponde nei commenti o in chat ricade nel paragrafo 1 dello stesso articolo, quello sull'interazione, e va dichiarato anche quando nessun contenuto è generato.

Fondamento: articolo 50, paragrafi 1, 4 e 5; orientamenti della Commissione del 20 luglio 2026 · **Grado:** orientamento
Resta incerto dove passi il confine dell'interesse pubblico per un profilo aziendale. Un post che presenta un prodotto non informa il pubblico su una questione collettiva, mentre una presa di posizione su una consultazione, su un tema sanitario o ambientale ci si avvicina molto, e nessuna fonte consultata traccia la linea. Finché non lo fa, il criterio prudente che suggeriamo è guardare alla funzione del testo: se il lettore lo userebbe per formarsi un'opinione su una questione che riguarda tutti, trattatelo come tale.
Fondamento: nessuna fonte primaria né orientamento sul punto · **Grado:** aperta

D4. Che cosa si scrive esattamente sulle immagini e nei testi? Esistono formule standard?

Sì, esistono, e sono due sole. Prima però conviene sapere che cosa sia esattamente lo strumento che le stabilisce, perché il nome trae in inganno.
Il Codice di buone pratiche sulla trasparenza dei contenuti generati dall'IA è un atto europeo, non italiano: è stato elaborato sotto la regia dell'Ufficio per l'IA della Commissione, con il contributo di esperti indipendenti e degli operatori del settore, e pubblicato nella versione definitiva il 10 giugno 2026.
Il suo fondamento sta nell'articolo 50, paragrafo 7, dell'AI Act, che affida all'Ufficio per l'IA il compito di incoraggiare e agevolare l'elaborazione di codici di buone pratiche europei proprio per rendere praticabili gli obblighi di rilevazione ed etichettatura dei contenuti artificiali.
Nella gerarchia delle fonti del capitolo 2 il Codice sta al quarto livello, quello della soft law: sotto i regolamenti e gli atti di esecuzione, sopra nulla di vincolante. Non è una norma e nessuno può essere sanzionato per non averlo seguito; l'adesione è volontaria e alla fine di luglio 2026 lo avevano sottoscritto circa 190 fra imprese e organizzazioni. Vale però quanto il § 2.4 dice per l'intera categoria: è il metro che le autorità useranno concretamente per valutare i comportamenti, e aderirvi è il modo più semplice per dimostrare la conformità.
Il Codice mette quindi a disposizione un set di icone europee liberamente utilizzabili, con due sole diciture: AI GENERATED per i contenuti creati da zero e AI MODIFIED per i contenuti reali ritoccati con l'IA. Le icone esistono in quattro varianti, due piene e due al 50% di trasparenza, in nero e in bianco, e si scaricano gratuitamente in SVG e PNG dalla pagina della Commissione dedicata alle icone UE per l'etichettatura dei contenuti generati dall'IA; il testo del Codice sta su una pagina distinta dello stesso sito. Gli indirizzi completi sono in fondo a questa risposta. In alternativa si possono usare etichette equivalenti, purché rispettino le specifiche di design, collocazione e accessibilità che il Codice fissa nella sezione 2.
Attenzione a un punto che cambia tutto: l'uso delle icone è facoltativo, mentre l'obbligo dell'articolo 50 non lo è. Chi preferisce una formula propria resta libero di scriverla, a patto che il risultato sia altrettanto chiaro; chi adotta le icone, invece, ha dalla sua uno strumento riconoscibile e già valutato dalla Commissione.
Fondamento: articolo 50, paragrafo 7, dell'AI Act per il fondamento del Codice · **Grado:** testo normativo. Contenuto del Codice di buone pratiche del 10 giugno 2026 e set di icone · **Grado:** orientamento
La distinzione fra le due diciture segue la stessa linea che l'articolo 50 traccia con l'espressione «generato o manipolato», e non ammette una terza via.

Che cosa avete pubblicato	Dicitura	Perché quella
Immagine, video o audio creati interamente con l'IA	AI GENERATED	Il contenuto non esisteva prima: è generato
Fotografia o video reali su cui l'IA ha aggiunto, tolto o alterato elementi	AI MODIFIED	Il contenuto esisteva: è manipolato
Voce sintetica che riproduce una persona reale su una base registrata	AI MODIFIED	La registrazione esiste, la voce è alterata
Testo di interesse pubblico scritto interamente dall'IA	AI GENERATED	Vale la stessa logica dei contenuti visivi

Una formula come "parziale uso dell'IA" o "realizzato con il supporto dell'IA" non esiste nel Codice, e conviene evitarla: attenua la dichiarazione senza appoggiarsi a nulla, e chi legge non capisce se ha

davanti un contenuto autentico oppure no. Se il dubbio è fra le due diciture, la scelta prudente è AI GENERATED, che dichiara di più.
Fondamento: articolo 50, paragrafo 4, dell'AI Act per la coppia generato/manipolato; Codice di buone pratiche per le diciture · **Grado:** orientamento
Sulla collocazione il Codice è più preciso di quanto ci si aspetti, e sono le tre regole che in pratica si violano più spesso.

- Percepibile dal primo contatto. L'etichetta va vista appena il contenuto compare, non dopo un tocco, non aprendo la descrizione, non scorrendo la didascalia.
- In un punto libero. Va collocata dove nessun elemento dell'interfaccia le si sovrappone: sui social significa stare lontani dagli angoli occupati da pulsanti, contatori, barre di avanzamento e titoli, che cambiano da piattaforma a piattaforma.
- Deve sopravvivere alla ricondivisione. Il Codice chiede che l'icona sia incorporata nel contenuto stesso e resti visibile anche quando il materiale viene ricondiviso o scaricato. È la conferma tecnica di quanto detto in D3: la didascalia si perde per strada, il pixel no.

Fondamento: Codice di buone pratiche, requisiti di visibilità e accessibilità · **Grado:** orientamento
Vediamo come si traduce in pratica, caso per caso.

- Post con immagine generata. Icona AI GENERATED nell'angolo alto dell'immagine, più una riga in apertura di didascalia: «Immagine generata con intelligenza artificiale.» La ridondanza non è uno spreco, perché copre il caso in cui l'immagine venga ritagliata.
- Video con voce sintetica. Icona in sovraimpressione per i primi secondi e nei metadati del file, più la dichiarazione all'inizio della descrizione. Se la voce riproduce una persona reale, la dichiarazione va nel video, non solo accanto.
- Articolo di blog su una novità normativa scritta dall'IA. In apertura, prima del testo: «Questo articolo è stato generato con l'intelligenza artificiale e non è stato sottoposto a revisione editoriale.» Se invece la revisione c'è stata nei termini del § 6.1, la dichiarazione non serve, ma conviene indicare chi se ne assume la responsabilità.
- Assistente conversazionale. Al primo messaggio, prima che l'utente scriva: «Stai parlando con un assistente automatico.» Ricade nel paragrafo 1 dell'articolo 50, quindi vale sempre, anche senza contenuti generati.
- Contenuto satirico o di finzione. L'obbligo si assolve senza ostacolare la fruizione, per esempio nei titoli di coda o in una nota, e non con una scritta sovrimpressa per tutta la durata (§ 6.1).

Fondamento: articolo 50, paragrafi 1, 4 e 5; Codice di buone pratiche · **Grado:** orientamento

Resta una questione che nessuna fonte affronta: le diciture ufficiali sono in inglese, mentre l'articolo 50 chiede che l'informazione sia chiara per chi la riceve. Su un pubblico italiano generalista AI GENERATED potrebbe non essere immediato quanto sembra a chi lavora nel settore. Il Codice ammette etichette equivalenti conformi alle sue specifiche, quindi la strada c'è; noi suggeriamo di affiancare l'icona europea a una riga in italiano, così da avere insieme il segno riconoscibile in tutta l'Unione e la comprensibilità per il vostro lettore.
Fondamento: nessuna fonte sul requisito linguistico; lettura sistematica dell'articolo 50, paragrafo 5 · **Grado:** aperta
Dove trovarli. Le due pagine ufficiali della Commissione europea, con gli indirizzi per esteso.

- Icone UE per l'etichettatura dei contenuti generati dall'IA: https://digital-strategy.ec.europa.eu/en/policies/eu-icons-labelling-ai-generated-content
- Codice di buone pratiche sulla trasparenza dei contenuti generati dall'IA: https://digital-strategy.ec.europa.eu/en/policies/code-practice-ai-generated-content

D5. Se il cliente consegna all'agenzia immagini o video fatti con l'IA senza dirlo, l'agenzia risponde di qualcosa?

Dipende da che cosa fa l'agenzia con quel file, e la distinzione è netta.
Se l'agenzia si limita a ricevere il materiale e a pubblicarlo, l'obbligo dell'articolo 50 non la raggiunge. Il paragrafo 4 grava sui deployer di un sistema di IA che genera o manipola il contenuto, e chi riceve un file già pronto non ha usato alcun sistema: l'utilizzatore, nel senso dell'articolo 3, numero 4, è il cliente che ha generato l'immagine sotto la propria autorità. Gli orientamenti della Commissione confermano la lettura dal lato opposto, escludendo dagli obblighi di trasparenza chi si limita a ospitare o distribuire contenuti altrui.
Se invece l'agenzia mette mano al contenuto con strumenti propri, e capita più spesso di quanto sembri, la posizione cambia. Un ampliamento generativo dell'inquadratura, una sostituzione di sfondo, un ritocco automatico, un doppiaggio sintetico: sono tutte manipolazioni compiute con un sistema di IA sotto l'autorità dell'agenzia, che diventa così utilizzatore per la propria parte. L'obbligo nasce dall'atto, non dalla consapevolezza: il fatto di ignorare l'origine del file ricevuto non toglie nulla, perché l'agenzia risponde di ciò che ha fatto lei.
Fondamento: articolo 3, numero 4, e articolo 50, paragrafo 4, dell'AI Act; orientamenti della Commissione del 20 luglio 2026 per l'esclusione di chi ospita o distribuisce · **Grado:** testo normativo e orientamento

Nessuna delle fonti consultate affronta però il caso dell'agenzia in buona fede, e le due conclusioni qui sopra sono una lettura sistematica delle definizioni, non una presa di posizione che possiamo citare. Su un punto la lettura è comunque solida: la buona fede non crea e non estingue l'obbligo, semmai incide sulla misura della sanzione, perché il carattere doloso o colposo della violazione è fra i criteri che le autorità considerano nel quantificarla (§ 11.1).
Fondamento: nessuna fonte sul caso specifico · **Grado:** aperta

Anche quando l'articolo 50 non affronta l'argomento, l'agenzia resta esposta su tre fronti che con l'AI Act non hanno nulla a che vedere.

- Il rapporto con il cliente. Se la contestazione arriva e il contratto tace, l'agenzia non ha su cosa appoggiarsi per rivalersi, e si trova a discutere di un obbligo altrui con i propri mezzi.
- I canali propri. Un lavoro ripubblicato nel portfolio, in un caso studio o sui profili dell'agenzia non è più diffusione per conto del cliente: lì a diffondere è l'agenzia, e la valutazione si rifà da capo con lei al posto del cliente.
- La correttezza commerciale. Presentare al pubblico come autentico un contenuto che non lo è può rilevare anche sul piano delle pratiche commerciali, che seguono regole proprie e un'autorità diversa. È un terreno su cui non abbiamo fonti, e lo segnaliamo come possibilità da verificare con un legale.

Fondamento: nessuna fonte primaria; ricostruzione per analogia · **Grado:** aperta
Il rimedio, come quasi sempre in questa materia, è contrattuale e costa poche righe. Nel contratto di fornitura o nell'ordine conviene chiedere al cliente una dichiarazione sull'uso dell'IA nei materiali consegnati, distinguendo fra contenuti generati e contenuti modificati secondo la coppia di D4, una garanzia sull'esattezza di quella dichiarazione e l'impegno a tenere indenne l'agenzia da contestazioni che ne derivino. Sono le stesse clausole che il § 8.6 raccomanda in senso inverso, quando è l'impresa a doversi tutelare verso il proprio fornitore, e alla fine il presidio è lo stesso letto dall'altro capo del tavolo.
Sul piano operativo basta una domanda in fase di consegna, registrata per iscritto: quali materiali sono stati prodotti o modificati con l'IA. Una risposta scritta vale come evidenza, e riporta l'onere su chi quell'informazione la possiede.
Fondamento: § 8.6 della guida; nessuna fonte normativa impone questa clausola · **Grado:** aperta

D6. E se è l'agenzia a usare l'IA senza dirlo al cliente? In caso di controllo chi risponde?

È il caso speculare rispetto a D5, e l'esito si rovescia: qui a usare il sistema sotto la propria autorità è l'agenzia, quindi l'obbligo dell'articolo 50 è suo. Che il contenuto esca sui canali del cliente e porti il marchio del cliente non sposta la qualifica, perché l'articolo 3, numero 4, guarda a chi impiega il sistema e non a chi appare in firma. Il fatto di non averlo detto al committente non attenua nulla nei confronti dell'autorità: è una questione fra le due imprese, non fra l'agenzia e la vigilanza.
Fondamento: articolo 3, numero 4, e articolo 50, paragrafo 4, dell'AI Act · **Grado:** testo
La ripartizione che la pratica sta adottando è che ciascuno risponde della propria parte: l'agenzia per i sistemi che gestisce e per i contenuti che produce, il cliente per i sistemi che amministra in proprio e per i canali su cui pubblica. È una lettura ragionevole e coerente con le definizioni, ma va detto che la troviamo in fonti di settore e non in un atto della Commissione, quindi non poggia su nulla che possiamo citare come vincolante.
Fondamento: fonti secondarie di settore; nessun atto che ripartisca espressamente fra committente e fornitore · **Grado:** aperta
C'è però uno scarto fra chi risponde in diritto e chi si trova davanti l'ispezione, ed è il punto che rende questa domanda diversa dalla precedente. Il primo interlocutore dell'autorità è il marchio, perché è quello che il pubblico vede: sarà l'impresa committente a ricevere la richiesta di informazioni, e per spostare la posizione dovrà dimostrare chi ha prodotto che cosa e con quali strumenti. Se l'agenzia non l'ha mai dichiarato, quella prova l'impresa non ce l'ha, e si difende da una contestazione altrui senza gli elementi per farlo.
In D5 chi ignorava era protetto dal non aver usato alcun sistema; qui chi ignora è esposto proprio perché il contenuto porta il suo nome. L'ignoranza tutela chi sta a valle della produzione e lascia scoperto chi sta a valle della pubblicazione.
Fondamento: nessuna fonte sul caso; il criterio del carattere doloso o colposo nella quantificazione resta quello dell'articolo 99 (§ 11.1) · **Grado:** aperta
Sul piano del rapporto fra le due imprese l'agenzia che tace è in una posizione fragile su tre fronti.

- L'inadempimento contrattuale. Il mandato professionale impone di informare il committente delle modalità di esecuzione, e l'uso di un sistema generativo su materiali destinati alla pubblicazione è una di quelle.
- La rivalsa. Se il cliente subisce una contestazione o un danno reputazionale, la strada per rifarsi sull'agenzia è aperta, e il silenzio pesa contro chi lo ha tenuto.
- La perdita dell'esenzione editoriale. Per i testi di interesse pubblico l'esenzione del § 6.1 richiede una revisione umana con assunzione di responsabilità editoriale: se il cliente non sa che il testo è generato, non può assumersi nulla, e l'esenzione non si forma per nessuno dei due.

Fondamento: § 6.1 per l'esenzione editoriale; ricostruzione per il resto · **Grado:** aperta

Il presidio è lo stesso di D5 letto al contrario, e conviene a entrambe le parti. L'agenzia dichiara nel contratto o nella nota di consegna quali materiali sono stati prodotti o modificati con l'IA, e il cliente inserisce l'obbligo di quella dichiarazione fra le clausole minime del § 8.6. Per l'agenzia quella dichiarazione non toglie nulla e aggiunge parecchio, perché fa constare per iscritto ciò che ha fatto, che è anche l'unica difesa disponibile quando la contestazione arriva mesi dopo e nessuno ricorda più chi ha toccato quale file.
Fondamento: § 8.6 della guida; nessuna fonte normativa impone questa clausola · **Grado:** aperta

D7. Una policy interna sull'uso dell'IA ha valore legale in caso di controllo o contestazione?

Sì, ma non quello che di solito le si attribuisce. Una policy non crea esenzioni e non sostituisce alcun obbligo: se l'articolo 50 chiedeva una dichiarazione e la dichiarazione manca, averlo scritto in un documento interno non sana nulla. Il suo valore è probatorio, e si esercita su due terreni diversi, quello dell'adempimento e quello della misura della sanzione.

Sul primo terreno la policy è il modo con cui dimostrate di aver fatto ciò che il regolamento vi chiede in termini organizzativi. L'articolo 4 dell'AI Act, nella versione modificata dal Digital Omnibus, impone a fornitori e deployer di adottare misure adeguate a promuovere la formazione del personale sull'IA (§ 7.1): una policy scritta, con l'evidenza di averla diffusa e delle sessioni svolte, è quell'adempimento, non il suo racconto. Quando poi il sistema tratta dati personali entra in gioco anche il GDPR, che all'articolo 24, paragrafo 2, nomina espressamente l'attuazione di politiche adeguate fra le misure con cui il titolare dimostra la conformità.

Fondamento: articolo 4 dell'AI Act come modificato dal Reg. (UE) 2026/1744; articolo 24, paragrafo 2, del GDPR · **Grado:** testo normativo

Sul secondo terreno la policy incide quando la violazione c'è già stata. Fra i criteri con cui le autorità quantificano la sanzione figurano le misure adottate per attenuare il danno, il grado di cooperazione e il carattere doloso o colposo del fatto (§ 11.1): un presidio documentato parla a tutti e tre, e sposta la valutazione da una condotta trascurata a un incidente dentro un sistema che funzionava. È lo stesso principio che il § 11.3 ricava dai provvedimenti del Garante, dove ciò che viene contestato è quasi sempre la mancanza di procedure più che la tecnologia.

Fondamento: articolo 99 dell'AI Act per i criteri di quantificazione · **Grado:** testo

C'è però un rovescio che conviene conoscere prima di scriverla, ed è il motivo per cui una policy va presa sul serio o non va fatta. Una policy disattesa peggiora la posizione di chi l'ha scritta: dimostra che l'impresa conosceva il rischio, aveva individuato la regola e non l'ha applicata, il che trasforma una disattenzione in una scelta. Nessuna fonte lo afferma per l'AI Act, ma è il modo in cui funzionano i modelli organizzativi in generale, e in Italia lo si vede da vent'anni con i modelli 231.

Fondamento: nessuna fonte sul punto per l'AI Act; principio generale dei modelli organizzativi · **Grado:** aperta

Perché la policy regga davanti a un'autorità servono cinque cose, e sono tutte di forma.

- Una data e una versione. Un documento senza data non prova nulla, perché non si sa se esisteva prima del fatto contestato.
- Un'approvazione. Deve risultare chi l'ha adottata e con quale autorità, altrimenti resta un appunto di reparto.
- La prova della diffusione. Non basta averla scritta: serve l'evidenza che sia arrivata a chi lavora, con una ricevuta, una firma o un registro.
- La formazione documentata. Destinatari, contenuti, date e materiali, che è quanto il § 12.2 chiede già nella roadmap dei novanta giorni.
- Le tracce dell'applicazione. Le decisioni prese seguendo la policy, comprese quelle di non fare qualcosa, con le ragioni: sono la differenza fra un documento vivo e un documento esposto in bacheca.

Fondamento: § 11.1 e § 12.2 della guida; nessuna fonte impone questo elenco · **Grado:** aperta

Due innesti valgono la pena, se l'impresa ne dispone. Per le società dotate di modello organizzativo ex D.Lgs. 231/2001 la parte sull'IA va coordinata con quel modello, perché alcune fattispecie aggravate dall'uso dell'intelligenza artificiale possono rientrare nel catalogo dei reati presupposto (§ 9.3). E se la policy contiene divieti rivolti ai dipendenti, va ricordato che un comportamento si può sanzionare solo se la regola era conoscibile: sul piano del lavoro la diffusione non è un adempimento formale.

Fondamento: § 9.3 della guida per il rinvio al 231; principio generale in materia di lavoro · **Grado:** aperta

14. Dodici convinzioni diffuse da correggere

Si sente dire	In realtà
"L'AI Act riguarda solo le big tech."	Riguarda chiunque usi sistemi di IA nell'ambito di un'attività professionale. La categoria dei deployer comprende la quasi totalità delle imprese e degli studi professionali (§ 3.1).
"È tutto rinviato al 2027, non c'è fretta."	È rinviato solo il pacchetto sui sistemi ad alto rischio. Divieti, trasparenza, obblighi GPAI, sanzioni e vigilanza sono pienamente applicabili (capitolo 7).
"Se compro il software da un fornitore, la responsabilità è sua."	La responsabilità è ripartita. Il deployer ha obblighi propri e ne risponde in proprio; in alcuni casi assume addirittura gli obblighi del fornitore (§ 3.2).
"Basta essere conformi al GDPR."	Sono due discipline distinte, con autorità e sanzioni diverse, che si applicano cumulativamente (§ 10.1).
"Il consenso del dipendente legittima l'analisi delle emozioni."	No. Il riconoscimento delle emozioni sul luogo di lavoro è una pratica vietata: nessun consenso può renderla lecita (§ 4.1).
"Se il fornitore è extraeuropeo, l'AI Act non si applica."	Il regolamento si applica anche ai fornitori di Paesi terzi quando il sistema è immesso sul mercato UE o il suo output è utilizzato nell'Unione (§ 8.2).
"Basta scrivere in fondo alla pagina che usiamo l'IA."	L'informazione deve essere chiara, distinguibile e fornita al più tardi al momento della prima interazione o esposizione (§ 6.1).
"L'IA generativa per uso interno non ha vincoli."	Restano gli obblighi di alfabetizzazione, la tutela dei dati e del segreto, l'informativa ai lavoratori se incide sul rapporto di lavoro, e la responsabilità per gli output (§ 8.1).
"Il Codice di buone pratiche è obbligatorio."	L'adesione è volontaria. Sono gli obblighi dell'articolo 50 a essere vincolanti: il Codice è uno dei modi per dimostrare di rispettarli (§ 2.4).
"Le immagini e i testi che genero con l'IA sono roba mia."	Un contenuto interamente generato, senza apporto creativo umano riconoscibile, non gode di protezione: nessuna esclusiva, e chiunque può riutilizzarlo (§ 9.2).
"Sul piano civile non cambia nulla."	Dal 9 dicembre 2026 software e sistemi di IA sono prodotti ai fini della responsabilità da prodotto difettoso, con onere della prova alleggerito per chi agisce (§ 11.2).
"Nessuno controllerà davvero."	Dal 2 agosto 2026 le autorità di vigilanza hanno pieni poteri ispettivi e sanzionatori. E il controllo non è un'ipotesi futura: il Garante privacy ha già sanzionato (§ 11.3).

15. Glossario essenziale

Termine	Significato
Sistema di IA	Sistema automatizzato progettato per funzionare con livelli di autonomia variabili, che può presentare adattività dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dagli input ricevuti come generare output (previsioni, contenuti, raccomandazioni o decisioni) capaci di influenzare ambienti fisici o virtuali (art. 3, n. 1; capitolo 4).
Fornitore (provider)	Persona fisica o giuridica, autorità pubblica, agenzia o altro organismo che sviluppa un sistema di IA o un modello per finalità generali, oppure lo fa sviluppare, e lo immette sul mercato o lo mette in servizio con il proprio nome o marchio, a titolo oneroso o gratuito. La qualifica non dipende dalla vendita: vi rientra anche l'impresa che costruisce uno strumento per uso interno e lo mette in servizio. È il ruolo che porta il carico di obblighi più pesante del regolamento (art. 3, n. 3; § 3.1).
Deployer (utilizzatore)	Persona fisica o giuridica, autorità pubblica, agenzia o altro organismo che utilizza un sistema di IA sotto la propria autorità nell'ambito di un'attività professionale; resta fuori l'uso personale non professionale. È il ruolo in cui ricade la quasi totalità delle imprese e degli studi, e comporta obblighi propri, che non derivano da quelli del fornitore e non si estinguono con l'adempimento altrui. Chi personalizza un sistema di terzi, lo rimarchia o ne muta la finalità prevista può assumere gli obblighi del fornitore (art. 3, n. 4, e art. 25; § 3.1 e § 3.2).
Modello GPAI	Modello di IA per finalità generali: addestrato su grandi quantità di dati, capace di svolgere un'ampia gamma di compiti distinti e di essere integrato in sistemi diversi (§ 4.5).
Rischio sistemico	Rischio specifico delle capacità di impatto elevato dei modelli GPAI, con effetti potenzialmente significativi sul mercato interno, sulla salute pubblica, sui diritti fondamentali o sulla società (§ 4.5).
Contenuto sintetico	Contenuto audio, video, immagine o testo generato o manipolato mediante un sistema di IA (§ 6.1).
Deepfake	Contenuto generato o manipolato con l'IA che ritrae persone, oggetti, luoghi o eventi in modo da apparire falsamente autentico o veritiero (§ 6.1).
Formato leggibile meccanicamente	Marcatura che consente a un software di riconoscere l'origine artificiale di un contenuto: filigrane digitali, metadati, identificativi crittografici (§ 6.1).
Sorveglianza umana	Presidio umano sul funzionamento del sistema, esercitato da persone competenti con l'autorità e gli strumenti per interpretare gli output, disattivare il sistema o non seguirne le indicazioni (§ 8.1).
FRIA	Valutazione d'impatto sui diritti fondamentali, richiesta a determinati deployer di sistemi ad alto rischio prima della messa in servizio (art. 27; § 8.5).
Norma armonizzata	Specifica tecnica europea la cui applicazione fa presumere la conformità ai requisiti del regolamento (§ 2.3).

Termine	Significato
Organismo notificato	Soggetto indipendente designato per svolgere le valutazioni di conformità dei sistemi ad alto rischio nei casi previsti (§ 8.2).
Sandbox regolamentare	Spazio controllato di sperimentazione, sotto la supervisione dell'autorità competente, in cui sviluppare e testare sistemi innovativi prima dell'immissione sul mercato (§ 6.3).
Ufficio per l'IA	Struttura della Commissione europea competente sui modelli GPAI e sul coordinamento dell'attuazione del regolamento (§ 8.3).
Estrazione di testi e dati (TDM)	Analisi automatizzata di grandi quantità di testi, immagini o dati per ricavarne informazioni, tipicamente per addestrare un modello. È consentita entro limiti precisi, e il titolare dei diritti può riservarsene l'utilizzo (§ 9.2).
Riserva sull'estrazione (opt-out)	Dichiarazione con cui il titolare dei diritti esclude che le proprie opere siano usate per l'estrazione di testi e dati. Per i contenuti online va espressa in forma leggibile automaticamente, perché sia opponibile (§ 9.2).
Clausole contrattuali tipo	Modelli di clausole predisposti dalla Commissione europea per l'acquisto di sistemi di IA, in versione per sistemi ad alto rischio e non. L'adozione è volontaria e non copre proprietà intellettuale, corrispettivi e responsabilità contrattuale generale (§ 8.6).
Responsabilità da prodotto	Regime di responsabilità oggettiva del produttore verso chiunque subisca un danno da un prodotto difettoso, indipendentemente da un rapporto contrattuale. Dal 9 dicembre 2026 comprende espressamente software e sistemi di IA (§ 11.2).
Shadow AI	Strumenti di intelligenza artificiale adottati autonomamente da singole persone o funzioni aziendali, senza passare da una valutazione dell'IT o del legale. Sono la principale fonte di sorprese in sede di inventario (§ 12.1).
Accountability	Principio per cui non basta essere conformi: occorre poterlo dimostrare con documentazione, tracciabilità e decisioni motivate. Percorre sia il GDPR sia l'AI Act, e incide sulla quantificazione delle sanzioni (capitolo 12).

16. Le fonti citate, in ordine gerarchico

Diritto primario dell'Unione

- Trattato sul funzionamento dell'Unione europea, in particolare artt. 16 e 114.
- Carta dei diritti fondamentali dell'Unione europea.

Regolamenti dell'Unione europea

- Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale (AI Act), in GUUE L del 12 luglio 2024; in vigore dal 1° agosto 2024.
- Regolamento (UE) 2026/1744, Digital Omnibus sull'intelligenza artificiale: approvato dal Parlamento europeo il 16 giugno 2026, adottato dal Consiglio il 29 giugno 2026, pubblicato in GUUE il 24 luglio 2026, in vigore dal 27 luglio 2026.
- Regolamento (UE) 2016/679 (GDPR).
- Regolamento (UE) 2023/2854 (Data Act).
- Regolamento (UE) 2022/2065 (Digital Services Act).
- Regolamenti settoriali richiamati dall'Allegato I dell'AI Act: (UE) 2017/745 sui dispositivi medici, (UE) 2023/1230 sulle macchine, (UE) 2023/988 sulla sicurezza generale dei prodotti.

Direttive dell'Unione europea

- Direttiva (UE) 2024/2853 del 23 ottobre 2024 sulla responsabilità per danno da prodotti difettosi, che include espressamente software e sistemi di intelligenza artificiale nella nozione di prodotto; termine di recepimento 9 dicembre 2026, si applica ai prodotti immessi sul mercato dopo tale data.
- Direttiva (UE) 2022/2555 (NIS2) in materia di misure per un livello comune elevato di cybersicurezza.

Soft law e standard

- Commissione europea, **Orientamenti sull'attuazione dell'articolo 50** del Regolamento (UE) 2024/1689 in materia di trasparenza, 20 luglio 2026. https://digital-strategy.ec.europa.eu/en/policies/guidelines-transparency-obligations
- **Codice di buone pratiche sulla trasparenza dei contenuti generati dall'IA**, versione definitiva del 10 giugno 2026, elaborato sotto la regia dell'Ufficio per l'IA ai sensi dell'articolo 50, paragrafo 7. Adesione volontaria, circa 190 sottoscrittori a fine luglio 2026. https://digital-strategy.ec.europa.eu/en/policies/code-practice-ai-generated-content
- **Icone UE per l'etichettatura dei contenuti generati dall'IA**, parte integrante della sezione 2 del Codice: diciture *AI GENERATED* e *AI MODIFIED*, quattro varianti, formati SVG e PNG. https://digital-strategy.ec.europa.eu/en/policies/eu-icons-labelling-ai-generated-content
- Codice di buone pratiche per i modelli di IA per finalità generali, luglio 2025, e relativi orientamenti della Commissione.
- Commissione europea, Orientamenti sulle pratiche vietate e sulla definizione di sistema di IA, febbraio 2025.
- Norme tecniche in corso di elaborazione da parte di CEN-CENELEC; norma ISO/IEC 42001 sui sistemi di gestione dell'IA.

Diritto nazionale italiano

- Legge 23 settembre 2025, n. 132, recante disposizioni e deleghe al Governo in materia di intelligenza artificiale, in vigore dal 10 ottobre 2025.
- Schemi di decreto legislativo attuativo della legge n. 132/2025, approvati in esame preliminare dal Consiglio dei Ministri il 10 giugno 2026; iter in corso, termine della delega 10 ottobre 2026.
- Legge 17 marzo 2026, n. 36 (legge di delegazione europea 2025), che delega al Governo il recepimento della direttiva (UE) 2024/2853.
- D.Lgs. 26 maggio 1997, n. 152, art. 1-bis, in materia di informativa ai lavoratori sui sistemi decisionali e di monitoraggio automatizzati.
- Legge 22 aprile 1941, n. 633, sulla protezione del diritto d'autore, come modificata dalla legge n. 132/2025 in materia di creazione umana dell'opera e di estrazione di testi e dati.
- Codice penale: nuova fattispecie in materia di diffusione illecita di contenuti generati o alterati con sistemi di intelligenza artificiale e aggravante comune per i reati commessi mediante IA, introdotte dalla legge n. 132/2025.
- D.Lgs. 8 giugno 2001, n. 231, per i profili di responsabilità amministrativa degli enti.

Provvedimenti e atti citati

- Garante per la protezione dei dati personali, provvedimento del 14 maggio 2026 in materia di sistemi di intelligenza artificiale nei luoghi di lavoro.
- Garante per la protezione dei dati personali, provvedimento del 3 luglio 2026 nei confronti di Character Technologies Inc.
- Garante per la protezione dei dati personali, provvedimento del dicembre 2024 nei confronti di OpenAI, e parere sugli schemi di decreto legislativo attuativo della legge n. 132/2025.
- Comitato europeo per la protezione dei dati e Garante europeo della protezione dei dati, parere congiunto n. 2/2026 sulla proposta di semplificazione del quadro normativo digitale.
- Commissione europea, clausole contrattuali tipo per l'acquisto di sistemi di intelligenza artificiale, versioni per sistemi ad alto rischio e non ad alto rischio.
- AgID, linee guida per il procurement di intelligenza artificiale nella pubblica amministrazione.

Autorità competenti in Italia

- Agenzia per la cybersicurezza nazionale (ACN), autorità di vigilanza del mercato.
- Agenzia per l'Italia digitale (AgID), autorità di notifica degli organismi di valutazione della conformità.
- Garante per la protezione dei dati personali, Banca d'Italia, CONSOB, IVASS, nei rispettivi ambiti di competenza.

Fonti consultate

Fonti secondarie utilizzate per verificare date, importi, stato dell'iter normativo e contenuti dei provvedimenti. Non sono fonti del diritto: dove il loro contenuto divergeva, si è dato conto della versione confermata da più fonti indipendenti o dal testo ufficiale. Consultate ad agosto 2026.

AI Act, applicazione e scadenze

- Il Sole 24 Ore, AI Act, dal 2 agosto debuttano la vigilanza e i doveri di trasparenza
  https://www.ilsole24ore.com/art/ai-act-2-agosto-debuttano-vigilanza-e-doveri-trasparenza-AJtYEMV
- Altalex, AI Act: che cosa cambia davvero dal 2 agosto 2026 per imprese e professionisti
  https://www.altalex.com/documents/2026/07/31/act-cambia-davvero-2-agosto-2026-imprese-professionisti
- Agenda Digitale, AI Act, obblighi dal 2 agosto: come adeguarsi
  https://www.agendadigitale.eu/sicurezza/ai-act-obblighi-dal-2-agosto-come-adeguarsi/
- PMI.it, AI Act dal 2 agosto 2026, obblighi in vigore e rinvii
  https://www.pmi.it/impresa/normativa/475371/intelligenza-artificiale-dal-2-agosto-nuove-regole-ue.html
- Diritto.it, AI Act e PA: obblighi e scadenze dal 2 agosto 2026
  https://www.diritto.it/ai-act-e-pa-obblighi-e-scadenze-dal-2-agosto-2026/
- Vega Engineering, AI Act: scadenze da rispettare e sanzioni previste
  https://www.vegaengineering.com/news/ai-act-tutte-le-scadenze-da-rispettare-dal-2025-al-2028/
- Studio Legale Stefanelli, AI Act e medical device: tutte le date da segnare in agenda
  https://www.studiolegalestefanelli.it/it/approfondimenti/ai-act-e-medical-device-tutte-le-date-da-segnare-in-agenda-anche-per-evitare-sanzioni
- Studio Legale Celotti, AI Act 2 agosto 2026: cosa è vero e cosa no
  https://www.studiolegale.celotti.net/ai-act-2-agosto-2026-cosa-e-vero-cosa-no/

Digital Omnibus sull'intelligenza artificiale, Regolamento (UE) 2026/1744

- Altalex, Il Digital Omnibus sull'Intelligenza Artificiale in GUUE: cosa cambia per le imprese
  https://www.altalex.com/documents/2026/07/27/digital-omnibus-intelligenza-artificiale-guue-cambia-imprese
- Diritto e Giustizia, Pubblicato il Regolamento Digital Omnibus
  https://www.dirittoegiustizia.it/dettaglio/16076950/pubblicato-il-regolamento-digital-omnibus-lue-semplifica-lai-act-senza-ridurne-le-tutele
- Federprivacy, Il Consiglio UE approva le modifiche alle norme sull'intelligenza artificiale
  https://www.federprivacy.org/informazione/primo-piano/digital-omnibus-il-consiglio-ue-approva-le-modifiche-alle-norme-relative-all-intelligenza-artificiale
- ADVANT Nctm, Digital Omnibus on AI: il Consiglio adotta il Regolamento di semplificazione
  https://www.advant-nctm.com/en/news/digital-omnibus-on-ai-il-consiglio-adotta-il-regolamento-di-semplificazione-dellai-act
- AI4Business, Cosa cambia per i sistemi ad alto rischio
  https://www.ai4business.it/intelligenza-artificiale/ai-act-cosa-cambia-con-il-digital-omnibus-approvato-dal-parlamento-ue/

- Agenda Digitale, Digital Omnibus AI, cosa cambia davvero per le imprese https://www.agendadigitale.eu/sicurezza/digital-omnibus-ai-cosa-cambia-davvero-per-le-imprese/
- Agenda Digitale, Digital Omnibus sull'AI: nuove regole per i sistemi ad alto rischio https://www.agendadigitale.eu/sicurezza/digital-omnibus-sullai-nuove-regole-per-i-sistemi-ad-alto-rischio/
- CityNext, AI Act, arriva l'Omnibus digitale: cosa cambia con il Regolamento (UE) 2026/1744 https://citynext.it/2026/07/25/ai-act-omnibus-digitale-regolamento-2026-1744-cosa-cambia/
- Laura Turini, AI Act e Digital Omnibus: le novità della semplificazione normativa https://lauraturini.substack.com/p/ai-act-e-digital-omnibus-le-novita-semplificazione-normativa
- Digitalic, Cosa è scattato davvero dal 2 agosto e cosa è slittato al 2027 https://www.digitalic.it/intelligenza-artificiale/ai-act-2-agosto-2026-digital-omnibus-cosa-cambia

Obblighi di trasparenza, articolo 50

- Altalex, Gli orientamenti della Commissione UE sulla trasparenza dei contenuti https://www.altalex.com/documents/news/2026/07/29/ai-gli-orientamenti-della-commissione-ue-sulla-trasparenza-dei-contenuti
- Altalex, Il Codice di buone pratiche sulla trasparenza dei contenuti dell'IA https://www.altalex.com/documents/2026/06/25/act-codice-buone-pratiche-trasparenza-contenuti-intelligenza-artificiale
- Agenda Digitale, Obblighi di trasparenza AI Act: cosa devono fare le aziende dal 2 agosto 2026 https://www.agendadigitale.eu/sicurezza/obblighi-di-trasparenza-ai-act-cosa-devono-fare-le-aziende-dal-2-agosto-2026/
- Paradigma, Obblighi di trasparenza dell'AI Act: linee guida UE https://www.paradigma.it/obblighi-trasparenza-ai-act-linee-guida-commissione-europea/
- NicFab, Le linee guida della Commissione europea sull'art. 50 dell'AI Act https://www.nicfab.eu/en/posts/ai-act-art50-guidelines/
- Byte.it, AI Omnibus in vigore: più tempo, ma non sulla trasparenza https://www.byte.it/ai-omnibus-in-vigore-leuropa-concede-piu-tempo-ma-non-abbassa-la-guardia-sulla-trasparenza/

Sanzioni e modelli per finalità generali

- Economyup, Dal 2 agosto scattano le sanzioni dell'AI Act https://www.economyup.it/innovazione/dal-2-agosto-scattano-le-sanzioni-dellai-act-cosa-cambia-davvero-per-linnovazione-aziendale/
- Studio Legale V·D·S, AI Act, dal 2 agosto le sanzioni fanno sul serio https://intercodex.net/ai-act-sanzioni-2-agosto-chi-rischia/
- Quotidianopiù, Obblighi di trasparenza e disposizioni sui modelli GenAI https://www.quotidianopiu.it/dettaglio/12007644/ai-act-dal-2-agosto-in-vigore-obblighi-di-trasparenza-e-disposizioni-sui-modelli-genai
- Cyberness, AI Act e modelli GPAI: obblighi dal 2025, sanzioni dal 2026 https://www.cyberness.it/ai-act-gpai-modelli-finalita-generali-obblighi/

Legge 132/2025 e decreti attuativi

- ADVANT Nctm, Il CdM approva in via preliminare i decreti attuativi della Legge n. 132/2025 https://www.advant-nctm.com/news-e-approfondimenti/ai-il-cdm-approva-in-via-preliminare-i-decreti-attuativi-della-legge-n-132-2025
- Altalex, Decreti attuativi legge AI 132/2025: governance e polizia predittiva https://www.altalex.com/documents/news/2026/06/01/intelligenza-artificiale-estate-calda-decreti-delegati
- ADR firm, I due schemi di decreto attuativo: governance e ricadute operative https://www.adrfirm.it/2026/07/17/i-due-schemi-di-decreto-attuativo-della-legge-n-132-2025-sullintelligenza-artificiale/
- Filodiritto, Responsabilità penale, civile e governance della PA https://www.filodiritto.com/i-decreti-attuativi-della-legge-n-1322025-sullintelligenza-artificiale-responsabilita-penale-civile-e-governance-della-pubblica-amministrazione
- CorCom, Dal Cdm ok ai decreti: governance ad AgID e ACN https://www.corrierecomunicazioni.it/digital-economy/intelligenza-artificiale-il-governo-vara-la-cornice-italiana-governance-ad-agid-e-acn/
- Econopoly, Il Sole 24 Ore, Cosa prevedono i decreti sull'AI approvati dal governo https://www.econopoly.ilsole24ore.com/2026/06/10/cosa-prevedono-i-decreti-sullai-approvati-dal-governo/
- Agenda Digitale, Il modello italiano alla prova dell'enforcement https://www.agendadigitale.eu/sicurezza/intelligenza-artificiale-il-modello-italiano-alla-prova-dellenforcement/
- AI4Business, Il Garante privacy chiede più tutele su dati e biometria https://www.ai4business.it/intelligenza-artificiale/ai-act-il-garante-privacy-chiede-piu-tutele-su-dati-e-biometria/

Diritto d'autore

- Studio Previti, Le novità in materia di diritto d'autore introdotte dalla Legge 132/2025
  https://www.previti.it/le-novita-materia-di-diritto-dautore-introdotte-dalla-legge-1322025
- Iusletter, Equilibrio tra innovazione tecnologica e protezione dei diritti d'autore
  https://iusletter.com/dalla-redazione/diritto-dellimpresa/diritto-dautore/legge-132-2025-equilibrio-tra-innovazione-tecnologica-e-protezione-dei-diritti-dautore/
- Osservatorio IP, La legge 132/2025 traccia i confini della nuova creatività umana
  https://www.osservatorio-ip.it/2025/10/02/intelligenza-artificiale-e-diritto-dautore-la-legge-132-2025-traccia-i-confini-della-nuova-creativita-umana/
- Studio Sottocasa, L'opera resta umana, ma la prova diventa decisiva
  https://www.studiosottocasa.it/2026/02/19/intelligenza-artificiale-e-diritto-dautore-dopo-la-legge-n-132-2025-lopera-resta-umana-ma-la-prova-diventa-decisiva/

Profili penali e rapporti di lavoro

- Altalex, L'art. 612-quater c.p. e la tutela penale contro i deepfake
  https://www.altalex.com/documents/news/2026/01/09/art-612-quater-cp-tutela-penale-contro-deepfake-lacuna-normativa-tipizzazione-legislativa
- Agenda Digitale, AI, non solo deepfake: tutti i rischi penali per cittadini e imprese
  https://www.agendadigitale.eu/sicurezza/ai-non-solo-deepfake-tutti-i-rischi-penali-per-cittadini-e-imprese/
- Lavorosì, Dal 10 ottobre scatta l'obbligo di informativa a lavoratori e clienti
  https://www.lavorosi.it/dal-10-ottobre-scatta-lobbligo-di-informativa-a-lavoratori-e-clienti-sullutilizzo-dell-ia/
- GDPR.it, Nuovi obblighi per i datori di lavoro
  https://www.gdpr.it/entrata-in-vigore-la-legge-132-2025-sullintelligenza-artificiale-nuovi-obblighi-per-i-datori-di-lavoro/

Responsabilità da prodotto difettoso, direttiva (UE) 2024/2853

- Canella Camaiora, La nuova disciplina UE della responsabilità da prodotto difettoso non trascura l'AI
  https://canellacamaiora.it/direttiva-ue-2024-2853-la-nuova-disciplina-ue-della-responsabilita-da-prodotto-difettoso-non-trascura-lai/
- RP Legal & Tax, Il nuovo regime della responsabilità per danno da prodotti difettosi
  https://www.rplt.it/direttiva-ue-2024-2853-il-nuovo-regime-della-responsabilita-per-danno-da-prodotti-difettosi/
- P&S Legal, Responsabilità dei prodotti IA e software
  https://www.pandslegal.it/insights/responsabilita-dei-prodotti-ai-novita-ue-2853
- SCLA, È entrata in vigore la Direttiva UE 2024/2853
  https://scla.it/responsabilita-per-danno-da-prodotto-difettoso-direttiva-ue-2024-2853/

Normative connesse: GDPR, Data Act, NIS2, DORA

- EDPB, Joint Opinion 2/2026 on the Digital Omnibus
  https://www.edpb.europa.eu/documents/legislative-opinion/edpb-edps-joint-opinion-22026-on-the-proposal-for-a-regulation-as_en
- Altalex, Digital Omnibus: il parere congiunto EDPB/EDPS n. 2/2026
  https://www.altalex.com/documents/2026/03/11/digital-omnibus-parere-congiunto-edpb-edps-n-2-2026
- IRPA, Digital Omnibus: semplificazione normativa o erosione dei diritti fondamentali?
  https://www.irpa.eu/digital-omnibus-semplificazione-normativa-o-erosione-dei-diritti-fondamentali/
- Federprivacy, Applicabile dal 12 settembre il Data Act
  https://www.federprivacy.org/informazione/primo-piano/data-act-il-nuovo-regolamento-europeo-sull-accesso-equo-ai-dati-e-sul-loro-utilizzo-applicabile-dal-12-settembre
- Agenda Digitale, Data Act: la guida pratica per capirlo e applicarlo
  https://www.agendadigitale.eu/mercati-digitali/data-act-guida-alle-nuove-regole-per-laccesso-e-luso-dei-dati-in-europa/
- ICT Security Magazine, NIS2 e D.Lgs. 138/2024: gli adempimenti 2026
  https://www.ictsecuritymagazine.com/articoli/nis2-e-d-lgs-138-2024/
- Namirial, Scadenze NIS2: cosa devono fare le imprese entro ottobre 2026
  https://focus.namirial.com/it/nis2-scadenze-e-obblighi-2026
- Banca d'Italia, Regolamento (UE) 2022/2554, DORA
  https://www.bancaditalia.it/media/approfondimenti/2024/regolamento-dora/index.html
- Diritto Bancario, Il testo del Regolamento DORA in GU UE
  https://www.dirittobancario.it/art/dora-il-testo-del-regolamento-ue-2022-2554-in-gu-ue/

Provvedimenti delle autorità

- Garante privacy, Provvedimento del 14 maggio 2026, IA nei luoghi di lavoro
  https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10255494

- Garante privacy, Provvedimento del 3 luglio 2026, Character Technologies
  https://www.garanteprivacy.it/garante/doc.jsp?ID=10269571
- Garante privacy, Comunicato stampa sulla sanzione a Character.AI
  https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10269594
- Garante privacy, Provvedimento su OpenAI, dicembre 2024
  https://www.gpdp.it/home/docweb/-/docweb-display/docweb/10085432
- Garante privacy, Parere sugli schemi di decreto legislativo attuativo
  https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10275606
- Garante privacy, Audizione del Presidente sull'esame dello schema di decreto
  https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10273842
- ANSA, Il Garante privacy sanziona Character.AI per 158mila euro
  https://www.ansa.it/sito/notizie/topnews/2026/07/09/il-garante-privacy-sanziona-character.ai-per-158mila-euro_d62a48c0-c217-4459-95a5-df1a1acb0e2b.html
- Confindustria Toscana Centro e Costa, IA e lavoro: il provvedimento del Garante
  https://confindustriatoscanacentroecosta.it/ia-e-lavoro-provvedimento-del-garante-privacy-rischio-di-ingerenza-nei-confronti-dei-lavoratori/

Acquisti e clausole contrattuali

- Commissione europea, Clausole contrattuali tipo per l'acquisto di IA, versione alto rischio
  https://public-buyers-community.ec.europa.eu/sites/default/files/2023-10/AI_Procurement_Clauses_template_High_Risk%20IT.pdf
- Commissione europea, Clausole contrattuali tipo, versione non alto rischio
  https://public-buyers-community.ec.europa.eu/sites/default/files/2023-10/AI_Procurement_Clauses_Template_NON_HIGH_RISK_IT.pdf
- AgID, Linee guida per il procurement di IA nella PA, in consultazione
  https://www.agid.gov.it/sites/agid/files/2026-03/LLGG%20procurement_per%20consultazione%20pubblica.pdf
- Altalex, Le linee guida per il procurement di IA nella pubblica amministrazione
  https://www.altalex.com/documents/2026/04/14/linee-guida-procurement-ia-pubblica-amministrazione
- Diritto al Digitale, Model Contractual Clauses for AI Procurement
  https://dirittoaldigitale.com/2025/05/08/model-contractual-clauses-for-ai-procurement/

Appendice: il calendario delle scadenze in una pagina

Estratto dell'orizzonte operativo, dal 2 agosto 2026 al 2 agosto 2028, pensato per essere stampato e tenuto a portata di mano. Il calendario dell'AI Act per esteso, comprese le fasi già decorse e quelle successive al 2028, è al capitolo 5; per le scadenze delle normative connesse, che il capitolo 5 non riporta, il rimando è nell'ultima colonna.

Data	Che cosa scatta	Chi deve agire	Dove leggerne
2 agosto 2026 *(già in vigore)*	Obblighi di trasparenza dell'art. 50: avviso di interazione con un'IA, marcatura dei contenuti sintetici, informativa su sistemi biometrici, dichiarazione dei deepfake. Piena operatività di vigilanza e sanzioni; ammende della Commissione ai fornitori di modelli GPAI.	Fornitori e deployer, cioè in pratica tutti	§ 6.1, § 6.2
12 settembre 2026	Data Act: i nuovi dispositivi connessi immessi sul mercato devono essere	Produttori di prodotti connessi	§ 10.2

Data	Che cosa scatta	Chi deve agire	Dove leggerne
	progettati in modo da consentire l'accesso ai dati generati.		
10 ottobre 2026	Termine per l'esercizio della delega: adozione definitiva dei decreti attuativi della legge italiana sull'IA, con le regole nazionali su procedimento sanzionatorio e competenze delle autorità.	Nessun adempimento diretto: da monitorare	§ 9.4
31 ottobre 2026	NIS2: attuazione delle misure di sicurezza di base per i soggetti inclusi nel perimetro.	Soggetti essenziali e importanti NIS2	§ 10.2
2 dicembre 2026	Entrano in vigore i due nuovi divieti introdotti dal Digital Omnibus. Scade il termine per applicare la marcatura tecnica ai sistemi generativi già immessi sul mercato prima del 2 agosto 2026.	Fornitori di sistemi generativi	§ 4.1, capitolo 5
9 dicembre 2026	Nuova disciplina della responsabilità da prodotto difettoso: software e sistemi di IA sono prodotti. Si applica ai prodotti immessi sul mercato da questa data.	Chi sviluppa o incorpora IA nei propri prodotti	§ 11.2
2 agosto 2027	Scade il periodo transitorio per i modelli GPAI immessi sul mercato prima del 2 agosto 2025.	Fornitori di modelli per finalità generali	§ 4.5, § 8.3
2 dicembre 2027	Obblighi sui sistemi ad alto rischio dell'Allegato III: selezione del personale, merito creditizio, istruzione, biometria, servizi essenziali. Gestione del rischio, governance dei dati, documentazione, sorveglianza umana, registrazione, valutazione d'impatto sui diritti fondamentali.	Fornitori e deployer di quei sistemi	§ 4.2, § 8.1, § 8.2
2 agosto 2028	Obblighi sui sistemi ad alto rischio incorporati in prodotti già regolati: dispositivi medici, macchine, giocattoli.	Fabbricanti di prodotti regolati	§ 4.2, § 8.2

Come leggerla

La prima riga non richiede un progetto: richiede una verifica, e può essere chiusa in poche settimane. Le ultime due richiedono un progetto, e i tempi tecnici di adeguamento sono di dodici-diciotto mesi: dicembre 2027 va affrontato entro la fine del 2026. Le righe intermedie riguardano solo alcune imprese, ma per quelle sono vincolanti quanto le altre.

Avvertenza. Questo documento riflette il quadro normativo alla data del 10 agosto 2026, ed è una data che conta: i decreti attuativi della legge n. 132/2025 sono in corso di adozione, il pacchetto europeo di semplificazione sui dati è ancora in discussione e le norme tecniche armonizzate sono in fase di elaborazione. Sulla natura di questo documento e sui suoi limiti si veda la Premessa.

Nueva York
Londres
París
Milán
Madrid
Miami
Ciudad de México
Rimini
Tbilisi
Dublín
Bogotá
Padua
Barcelona
Lisboa
Valencia
Mallorca