IA generativa e diritto d'autore

Allinea

Avvera Compliance Review

Marzo 2026

Allinea
Avvera Compliance Review
Marzo 2026

Memorizzazione e riproduzione di opere protette nei modelli AI

Un recente report tecnico ha evidenziato come alcuni modelli di intelligenza artificiale generativa siano in grado di riprodurre porzioni sostanziali di libri coperti da copyright "from memory", ossia senza accesso diretto al testo durante la fase di inferenza. Il punto non è la semplice citazione occasionale. Il punto è la capacità strutturale del modello di memorizzare e rigenerare contenuti protetti, con un livello di fedeltà tale da superare la soglia della mera similarità statistica. L'evento è tecnicamente rilevante. Ma è giuridicamente dirompente. Per gli AI developer, non si tratta di un tema accademico: si tratta di esposizione diretta a responsabilità legale.

" Il modello è un asset tecnico, ma anche una potenziale fonte di liability strutturale"

Dalla Performance alla Responsabilità:
Il Perimetro Regolatorio Europeo tra Copyright e AI Act

L'Unione Europea ha adottato un approccio regolatorio preciso sull'AI attraverso l'AI Act. Il regolamento introduce obblighi specifici per i modelli di uso generale (GPAI), con particolare attenzione a:

- trasparenza sulle fonti di addestramento;
- documentazione tecnica;
- gestione del rischio sistemico.

Il principio sottostante è chiaro: l'innovazione non è esente da accountability.
Parallelamente, il diritto d'autore europeo non è stato sospeso per l'addestramento dei modelli. Le eccezioni per text and data mining non equivalgono a una licenza universale. E se il modello è in grado di rigenerare contenuti sostanzialmente identici all'opera originale, il problema non è più solo l'input (training), ma l'output.
Il tema si colloca quindi all'intersezione tra:

- proprietà intellettuale;
- regolazione dell'AI;
- governance del rischio tecnologico.
- Per un AI developer, questo significa una cosa sola: il modello è un asset tecnico, ma anche una potenziale fonte di liability strutturale.

Il nodo giuridico: riproduzione non autorizzata

La capacità di un modello di riprodurre un'opera protetta può configurare:

- violazione del diritto di riproduzione;
- violazione del diritto di comunicazione al pubblico;
- concorso nella diffusione di contenuti protetti tramite piattaforme.

Il rischio non dipende dall'intenzione del developer, ma dall'effetto concreto dell'output. Se l'architettura del modello consente la rigenerazione sostanzialmente fedele di opere protette, l'argomento difensivo della "mera probabilità statistica" diventa fragile.

Gli obblighi dell'AI Act per modelli di uso generale

L'AI Act introduce per i provider di modelli GPAI obblighi specifici, tra cui:

- predisposizione di documentazione tecnica dettagliata;
- pubblicazione di un riassunto sufficientemente dettagliato dei contenuti utilizzati per l'addestramento;
- implementazione di politiche per il rispetto del diritto d'autore.

Memorizzazione e riproduzione di opere protette nei modelli AI

Questo ultimo punto è cruciale. Non è sufficiente dichiarare che il modello è stato addestrato su dati "pubblicamente disponibili". Occorre dimostrare:
- tracciabilità delle fonti;
- gestione delle richieste di opt-out;
- misure per ridurre il rischio di output illeciti.

Qui entra in gioco la governance del ciclo di vita del modello.

Il profilo privacy: quando nei dataset ci sono dati personali
Qualora nei dataset siano presenti dati personali, il tema si estende al GDPR.
In tal caso, il developer diventa titolare del trattamento per la fase di training e deve dimostrare:
- base giuridica adeguata;
- rispetto dei principi di minimizzazione e limitazione della finalità;
- misure tecniche e organizzative adeguate.

La capacità del modello di "memorizzare" contenuti aumenta il rischio di:
- data leakage;
- ricostruzione di informazioni personali;
- violazioni del principio di integrità e riservatezza.

Il rischio non è solo IP. È anche data protection.

"Le piattaforme devono gestire contenuti illegali, inclusi quelli che violano il copyright"

Il ruolo delle piattaforme e la distribuzione dell'output
Se l'output generato viene distribuito tramite piattaforme online, possono entrare in gioco anche gli obblighi del Digital Services Act. Le piattaforme devono gestire contenuti illegali, inclusi quelli che violano il copyright. Se l'AI genera contenuti illeciti in modo sistemico, il rischio di escalation regolatoria è concreto. Per il developer, questo significa esposizione indiretta e pressioni contrattuali da parte dei distributori.

Dalla Teoria alla Liability: Mappatura dei Rischi per l'AI Developer
Per un AI developer, la questione si traduce in quattro aree di rischio:

Rischio legale diretto
- Azioni per violazione del copyright.
- Contenzioso transfrontaliero.
- Possibili sanzioni amministrative in ambito AI Act.

Rischio regolatorio
- Richieste di documentazione da parte delle autorità.
- Obblighi di dimostrare conformità strutturale.
- Necessità di audit tecnici indipendenti.

Rischio reputazionale
- Perdita di fiducia da parte di partner e clienti enterprise.
- Esclusione da procurement pubblici o corporate.

Rischio contrattuale
- Clausole di indennizzo richieste dai clienti.
- Limitazioni d'uso imposte dai distributori.

Memorizzazione e riproduzione di opere protette nei modelli AI

Azioni correttive e best practice
Un developer che vuole essere compliance-ready deve implementare:

1. Data governance strutturata
- Mappatura delle fonti.
- Log delle fasi di training.
- Politiche di esclusione contenuti protetti.

2. Test di memorization e leakage
- Red teaming specifico su copyright.
- Analisi di probabilità di riproduzione testuale.

3. Meccanismi di mitigazione
- Filtri di output.
- Fine-tuning mirato per ridurre rigenerazione fedele.
- Prompt injection control.

4. Documentazione AI Act compliant
- Dossier tecnico aggiornato.
- Sintesi pubblica delle fonti.
- Politiche interne di rispetto IP.

5. Framework di accountability
- Ruoli e responsabilità chiari.
- Supervisione legale nel ciclo di sviluppo.
- Integrazione tra team tecnico e legale.

La compliance non può essere un layer aggiunto ex post.
Deve essere integrata nel design.

"La compliance non può essere un layer aggiunto ex post. Deve essere integrata nel design"

Dalla Performance Tecnica alla Governance Documentata:
La Compliance come Vantaggio Competitivo
La capacità dei modelli di riprodurre libri protetti non è un bug marginale. È un indicatore di maturità tecnica che si trasforma in vulnerabilità giuridica. L'AI Act non vieta l'innovazione. Ma impone una cosa precisa: responsabilità strutturale.
Per gli AI developer europei – e per chi opera nel mercato UE – il vero spartiacque non sarà la performance del modello, ma la sua governance documentata.
La tendenza futura è chiara:
- maggiore scrutinio sui dataset;
- richieste di trasparenza sulle fonti;
- standardizzazione di audit di memorization;
- integrazione tra diritto d'autore e regolazione AI.

L'imperativo strategico è uno solo: trasformare la compliance da costo difensivo a vantaggio competitivo._Nel mercato europeo, la fiducia regolatoria diventerà una metrica di qualità tecnologica. I modelli che non sapranno dimostrare accountability non saranno semplicemente rischiosi, saranno non sostenibili.

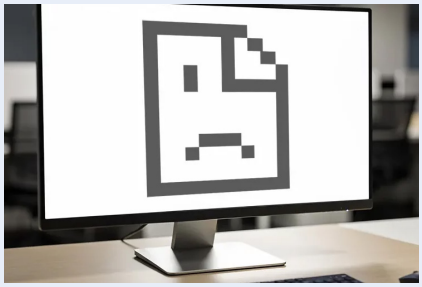
Allinea
Avvera Compliance Review
Marzo 2026

Attacco DDoS a Register.it

Migliaia di siti web inaccessibili per ore, clienti furiosi sui social, comunicazioni ufficiali affidate a post su Facebook. L'attacco subito da Register.it - uno dei principali registrar e provider di hosting italiani - offre uno spaccato preciso di cosa accade quando un'infrastruttura critica viene colpita da un attacco informatico su larga scala. E solleva domande che non riguardano solo la tecnologia, ma anche le responsabilità giuridiche di chi gestisce servizi digitali essenziali per migliaia di imprese.

Cos'è un attacco DDoS al DNS e perché è così devastante

L'acronimo DDoS sta per Distributed Denial of Service: un attacco che mira a rendere un servizio irraggiungibile saturando le sue risorse con un volume abnorme di richieste provenienti da fonti distribuite. In questo caso, il bersaglio era il DNS - il Domain Name System - ovvero il sistema che traduce i nomi di dominio (come "iltuosito.it") negli indirizzi IP necessari ai browser per raggiungere i server. Colpire il DNS significa, in pratica, abbattere le fondamenta dell'intera infrastruttura: anche se i siti e i server dei clienti sono perfettamente funzionanti, diventano semplicemente irraggiungibili.



"Colpire il DNS significa abbattere le fondamenta dell'intera infrastruttura"

Le responsabilità giuridiche del provider

Dal punto di vista legale, il caso solleva almeno tre ordini di questioni.
Il primo riguarda il contratto di servizio. I clienti di Register.it pagano - spesso anticipatamente - per garantire la disponibilità continuativa del proprio sito web. L'interruzione del servizio per cause imputabili a carenze nelle misure di sicurezza del provider potrebbe configurare un inadempimento contrattuale, con conseguente diritto al risarcimento del danno. La distinzione rilevante è tra l'attacco in sé - evento terzo e in linea di principio imprevedibile - e l'inadeguatezza delle contromisure adottate. Un provider di grandi dimensioni, che opera su scala nazionale, è ragionevolmente tenuto a disporre di sistemi di mitigazione DDoS proporzionati alla propria esposizione. Il secondo profilo riguarda la normativa sulla sicurezza informatica. Il Decreto Legislativo 138/2024, che recepisce la Direttiva NIS2, impone ai soggetti qualificabili come "essenziali" o "importanti" - categoria nella quale possono rientrare i grandi provider di servizi internet - obblighi precisi in materia di gestione del rischio e di notifica degli incidenti significativi all'Agenzia per la Cybersicurezza Nazionale (ACN) entro 24 ore dalla rilevazione. L'omessa o tardiva notifica espone a sanzioni amministrative rilevanti. Il terzo profilo attiene alla comunicazione. La scelta di Register.it di gestire l'emergenza esclusivamente attraverso i propri canali social - ritardando la comunicazione sulla homepage ufficiale - è giuridicamente problematica. Il GDPR e il Codice del Consumo impongono standard di trasparenza verso gli utenti che non si esauriscono in un post su Facebook. Comunicazioni tempestive, ufficiali e adeguatamente dettagliate non sono solo buona prassi: in certi contesti sono un obbligo.

Cosa insegna questo caso

L'incidente di Register.it ricorda che la resilienza informatica non è una questione puramente tecnica. È anche una questione di governance, di procedure e di obblighi normativi. Le imprese che affidano la propria presenza digitale a un provider esterno dovrebbero verificare i livelli di servizio garantiti contrattualmente (i c.d. SLA), le misure di sicurezza adottate e le procedure di incident response. E i provider, dal canto loro, devono considerare la cybersicurezza non come un costo opzionale, ma come un obbligo - nei confronti dei propri clienti, della normativa e del mercato.

Allinea
Avvera Compliance Review
Marzo 2026

Il bug Copilot
Quando l'AI ignora le etichette di riservatezza

Un bug in Microsoft 365 Copilot ha consentito, per un periodo limitato, il bypass delle policy di Data Loss Prevention (DLP), permettendo al sistema di intelligenza artificiale integrato nella suite Microsoft 365 di riassumere e processare email etichettate come "confidenziali". Non si è trattato di un attacco esterno né di un data breach nel senso tradizionale del termine. Il punto critico è diverso: l'AI ha trattato contenuti che, secondo le policy aziendali e le etichette di sensibilità, non avrebbero dovuto essere oggetto di elaborazione automatizzata. Il caso solleva un tema centrale di governance: quando l'AI è embedded nei processi aziendali, chi garantisce che rispetti effettivamente le policy di sicurezza e protezione dati già implementate?

AI Embedded e Compliance:
il punto di frizione tra innovazione e obblighi regolatori

L'episodio si colloca in un momento normativo estremamente denso. Il Regolamento (UE) 2016/679 impone al titolare del trattamento obblighi stringenti in materia di sicurezza (art. 32), accountability (art. 5.2) e protezione dei dati by design e by default (art. 25). Parallelamente, la Direttiva (UE) 2022/2555 rafforza i presidi di cybersecurity per soggetti essenziali e importanti, imponendo misure tecniche e organizzative adeguate e sistemi di gestione del rischio. A ciò si aggiunge il nuovo Regolamento (UE) 2024/1689, che introduce obblighi specifici di risk management e governance per i sistemi di IA, in particolare quelli integrati in contesti ad alto impatto. Il punto di frizione è evidente: le architetture DLP tradizionali sono state progettate per prevenire l'esfiltrazione o la condivisione indebita di dati, non per governare il trattamento interno da parte di sistemi generativi embedded. L'evento non è quindi solo tecnico. È un test di coerenza tra AI e compliance.

Profilo GDPR: sicurezza e accountability

Anche in assenza di accesso da parte di terzi non autorizzati, il trattamento di dati personali in violazione delle policy interne può configurare un problema di conformità.
Il GDPR impone che il trattamento sia:
- lecito, corretto e trasparente;
- limitato alle finalità;
- adeguatamente protetto mediante misure tecniche e organizzative appropriate.

Se un sistema AI elude le etichette di sensibilità e processa contenuti che l'organizzazione aveva classificato come non processabili, si pone un tema di:
- adeguatezza delle misure tecniche;
- effettiva implementazione del principio di privacy by design;
- tracciabilità e controllo del trattamento.

Il titolare resta responsabile. L'utilizzo di un vendor globale non attenua l'obbligo di accountability.

Profilo NIS2: gestione del rischio ICT

La NIS2 richiede un approccio strutturato alla gestione del rischio cyber.
Questo include:
- analisi delle vulnerabilità;
- controllo della supply chain digitale;
- monitoraggio continuo.

Il bug Copilot
Quando l'AI ignora le etichette di riservatezza

Un bug che consente il bypass di controlli DLP rientra nella categoria di vulnerabilità sistemiche. Anche se corretto rapidamente dal fornitore, l'organizzazione deve dimostrare:
- di aver valutato il rischio;
- di aver monitorato l'incidente;
- di aver aggiornato le proprie misure di sicurezza.

Il tema qui è la maturità del framework di governance ICT.

Profilo AI Act: affidabilità e controllo
L'AI Act introduce un principio chiave: i sistemi di IA devono essere progettati e utilizzati in modo da garantire un livello elevato di protezione dei diritti fondamentali.
Tra gli elementi centrali:
- gestione del rischio;
- trasparenza;
- supervisione umana;
- robustezza e sicurezza tecnica.

Un sistema che ignora le policy di sensibilità solleva interrogativi sulla robustezza del controllo ex ante e sulla capacità dell'organizzazione di esercitare una supervisione effettiva. L'AI embedded non è un semplice strumento. È un soggetto tecnologico che amplifica la superficie di rischio.

Riflessioni operative
Dal punto di vista della governance aziendale, il caso Copilot impone alcune riflessioni operative.

1. Audit delle integrazioni AI
Non è sufficiente abilitare Copilot o strumenti analoghi. È necessario:
- mappare i flussi informativi accessibili all'AI;
- verificare l'effettivo rispetto delle sensitivity label;
- testare scenari di bypass.

"L'AI embedded è un soggetto tecnologico che amplifica la superficie di rischio."

La compliance deve essere verificabile, non presunta.

2. Revisione dei contratti con i vendor
I contratti con fornitori di AI devono prevedere:
- obblighi di notifica tempestiva di vulnerabilità;
- SLA chiari sulle patch;
- clausole di responsabilità;
- accesso ai log per finalità di audit.

La supply chain digitale è parte integrante della governance.

3. Logging e tracciabilità
Un'organizzazione audit-ready deve poter dimostrare:
- quali dati sono stati processati dall'AI;
- in quale contesto;
- con quali controlli attivi.

Senza logging avanzato, l'accountability è puramente teorica.

Il bug Copilot
Quando l'AI ignora le etichette di riservatezza

4. DPIA e aggiornamento del risk register
Se l'AI è integrata in processi che coinvolgono dati personali, la Data Protection Impact Assessment deve essere aggiornata. Il risk register ICT deve includere:
- rischi di trattamento improprio interno;
- rischio reputazionale;
- rischio sanzionatorio.

L'assenza di data breach non equivale all'assenza di rischio.

Dalla produttività alla governance: l'AI come nuovo perimetro della responsabilità organizzativa
Il caso Copilot non dimostra che l'AI sia intrinsecamente insicura. Dimostra che l'integrazione dell'AI nei processi aziendali richiede un salto di paradigma nella governance. Le architetture di sicurezza tradizionali non sono state progettate per sistemi generativi che:
- accedono a repository trasversali;
- sintetizzano informazioni;
- generano output autonomi.

La vera questione non è il bug in sé. È la capacità dell'organizzazione di dimostrare controllo. In un contesto regolatorio sempre più stratificato – GDPR, NIS2, AI Act – la compliance non è un adempimento formale. È un framework dinamico di gestione del rischio tecnologico. L'adozione dell'AI deve essere accompagnata da un modello di governance integrato, documentato e verificabile. Non è più sufficiente chiedersi se l'AI migliori la produttività. Occorre chiedersi se l'organizzazione è strutturalmente pronta a governarla.

Allinea
Avvera Compliance Review
Marzo 2026

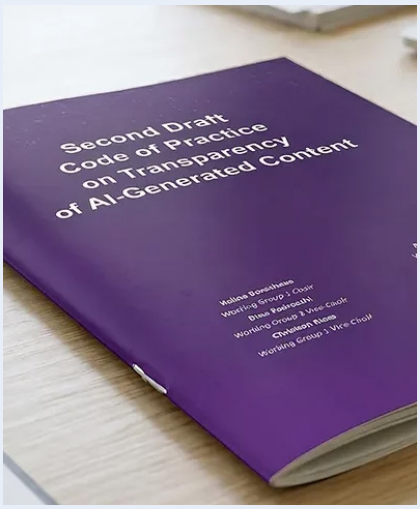
Etichettare l'IA
La commissione europea pubblica la seconda bozza del codice di condotta

Il 5 marzo 2026, la Commissione Europea ha pubblicato la seconda bozza del Code of Practice on Marking and Labelling of AI-generated content, il Codice di Condotta sulla marcatura e l'etichettatura dei contenuti generati dall'intelligenza artificiale. Si tratta di un passaggio cruciale nel percorso di attuazione dell'AI Act e, in particolare, degli obblighi di trasparenza previsti dall'articolo 50 del Regolamento (UE) 2024/1689.

Il contesto normativo: l'articolo 50 dell'AI Act
L'AI Act introduce obblighi differenziati in funzione del livello di rischio dei sistemi di intelligenza artificiale. Tra le disposizioni a carattere trasversale figura l'articolo 50, che impone specifici obblighi di trasparenza per i sistemi di IA generativa, con riguardo sia alla marcatura tecnica dei contenuti sintetici sia all'etichettatura dei cosiddetti deepfake. Queste regole diventeranno applicabili a partire dal 2 agosto 2026. Il Codice di Condotta in esame è uno strumento volontario, facilitato dalla Commissione, per supportare provider e deployer nell'adempimento di tali obblighi.

Etichettare l'IA

La commissione europea pubblica la seconda bozza del codice di condotta



La struttura del Codice: due sezioni, due destinatari

Il documento è articolato in due sezioni, ciascuna rivolta a soggetti diversi della filiera dell'IA generativa. La Sezione 1 è indirizzata ai provider di sistemi di IA generativa rientranti nell'ambito applicativo dell'articolo 50(2). Rispetto alla prima bozza, questa sezione è stata semplificata e resa più flessibile. Tra gli impegni principali spicca un approccio a due livelli per la marcatura: l'uso di metadati sicuri e tecniche di watermarking, con elementi facoltativi come il fingerprinting e il logging. L'obiettivo è promuovere standard aperti, abbattendo i costi di conformità per le imprese.

La Sezione 2 si rivolge invece ai deployer, ovvero ai soggetti che utilizzano sistemi di IA per produrre contenuti destinati al pubblico, con particolare attenzione ai deepfake e alle pubblicazioni su temi di pubblico interesse, ai sensi dell'articolo 50 (4). Rispetto alla prima bozza, è stata eliminata la tassonomia che distingueva i contenuti puramente generati dall'IA da quelli assistiti dall'IA. Restano tuttavia requisiti minimi di design e collocazione per icone, etichette e disclaimer, a garanzia di un livello uniforme di riconoscibilità per l'utente finale.

L'icona UE: un simbolo per l'IA sintetica

Un elemento di particolare interesse pratico è la proposta di una icona UE standardizzata, che i firmatari potranno utilizzare per segnalare la natura artificiale dei contenuti. La seconda bozza include in allegato esempi illustrativi di questo simbolo, che sarà discusso con gli stakeholder nei prossimi workshop. L'obiettivo è rendere disponibile gratuitamente uno strumento visivo uniforme e riconoscibile in tutta l'Unione, che semplifichi la comunicazione verso gli utenti e riduca i costi di compliance.

Il processo partecipativo e i prossimi passi

La seconda bozza è frutto di un ampio lavoro collegiale: i redattori indipendenti hanno integrato i contributi scritti di centinaia di stakeholder - industria, accademia e società civile - raccolti tramite un sondaggio europeo e attraverso incontri e workshop tenutisi nel gennaio 2026. Hanno contribuito anche gli Stati membri, tramite l'AI Board, e i membri del Parlamento Europeo, attraverso il gruppo di lavoro IMCO-LIBE. La Commissione raccoglierà feedback sulla seconda bozza fino al 30 marzo 2026, con l'obiettivo di finalizzare il Codice entro l'inizio di giugno 2026.

Cosa devono fare le imprese adesso

Le organizzazioni che sviluppano o utilizzano sistemi di IA generativa devono valutare con tempestività la propria posizione rispetto agli obblighi dell'articolo 50. L'adesione al Codice, benché volontaria, costituirà un importante segnale di conformità agli occhi delle autorità di vigilanza. In concreto, è opportuno avviare subito una mappatura dei sistemi di IA generativa in uso, verificare le soluzioni tecniche di marcatura già disponibili e monitorare gli sviluppi relativi all'icona UE. Soprattutto, vale la pena partecipare alla consultazione entro il 30 marzo 2026: è questa la sede in cui le imprese possono ancora influenzare la versione definitiva del Codice, prima che diventi il riferimento operativo per la compliance. La scadenza del 2 agosto 2026 si avvicina. Agire con anticipo è la scelta più prudente per ridurre l'esposizione a rischi sanzionatori e per costruire un rapporto di fiducia duraturo con utenti e autorità regolatorie.

Allinea
Avvera Compliance Review
Marzo 2026

Copilot Cowork e l'automazione delegata

Quando l'AI agisce per te, chi risponde?

Il 9 marzo 2026 Microsoft ha annunciato Copilot Cowork: uno strumento integrato in Microsoft 365 che consente di delegare all'AI l'esecuzione di task complessi - organizzare il calendario, preparare materiali per riunioni, condurre ricerche, costruire piani commerciali. Un agente che agisce: accetta meeting, modifica file, invia comunicazioni. Queste azioni producono effetti giuridicamente rilevanti. Il blog post ufficiale, comprensibilmente, non si sofferma su chi risponde quando qualcosa va storto. Sul piano contrattuale, l'utente che delega un task risponde delle sue conseguenze verso i terzi, esattamente come risponderebbe se avesse agito direttamente. L'AI non è un soggetto giuridico: chi autorizza l'azione ne è responsabile.

Sul piano regolatorio, l'AI Act - pienamente applicabile da agosto 2026 - introduce la figura del deployer: l'organizzazione che adotta il sistema AI in un contesto specifico. In ambito enterprise, il deployer non è Microsoft, ma l'impresa che usa Cowork. Con obblighi propri di valutazione del rischio, supervisione umana e documentazione della conformità. Cowork accede a email, file, riunioni e messaggi per eseguire i task assegnati. Microsoft garantisce che il sistema opera all'interno dei perimetri di sicurezza di Microsoft 365. Ma questo non chiude le questioni di data protection.

Quando l'AI elabora le email di un utente per preparare un briefing su un cliente, sta trattando dati personali di terzi. Qual è la base giuridica? Se tra quei dati figurano informazioni sensibili, si applica l'art. 9 GDPR. E se le azioni prodotte dal sistema hanno effetti significativi su persone fisiche, entra in gioco l'art. 22 sul divieto di decisioni basate esclusivamente su trattamento automatizzato. Il meccanismo di approvazione umana dichiarato da Microsoft è rilevante, ma deve essere sostanziale - non solo formale - per escludere il carattere pienamente automatizzato del trattamento. Microsoft dichiara di aver integrato la tecnologia di Anthropic (Claude) in Cowork, scegliendo il modello più adatto al compito tra provider diversi.
In una supply chain AI con più fornitori, la responsabilità tende a concentrarsi sul deployer finale - qui Microsoft - salvo rivalsa contrattuale verso i provider dei modelli sottostanti. È un profilo che il quadro regolatorio europeo non ha ancora risolto in modo granulare, ma i termini del problema sono già definiti.

Cosa bisognerà fare prima del deploy di tale soluzione:
- Condurre una DPIA sull'uso di Cowork, con focus sull'elaborazione automatizzata di dati personali in email e file.
- Verificare i Data Processing Agreement con Microsoft e accertarsi che l'elaborazione da parte di modelli di provider terzi sia contrattualmente regolata.
- Definire policy interne su quali categorie di dati possono essere trattate da sistemi automatizzati e quali restano fuori perimetro.
- Garantire che i checkpoint di approvazione umana siano effettivi e tracciabili, non solo formali.

Cowork è uno strumento potente. Ma nell'ecosistema regolatorio europeo, adottarlo significa assumere il ruolo di deployer - con responsabilità che non si esauriscono nell'accettare i termini di servizio di Microsoft.

Allinea
Avvera Compliance Review
Marzo 2026

Lombardia e Intelligenza Artificiale

Una legge regionale che guarda all'europa. I profili giuridici da tenere d'occhio

Il 2 marzo 2026 la Giunta regionale lombarda ha approvato all'unanimità la proposta di progetto di legge "Disposizioni in materia di ricerca, innovazione e intelligenza artificiale per lo sviluppo sostenibile", trasmettendola al Consiglio regionale per l'iter di approvazione. Si tratta di uno dei primi provvedimenti normativi regionali italiani che tenta di disciplinare in modo organico il sistema dell'intelligenza artificiale a livello territoriale, sostituendo la legge regionale 29/2016 "Lombardia è ricerca e innovazione" con un quadro aggiornato che recepisce il nuovo contesto europeo e nazionale - in particolare il Regolamento (UE) 2024/1689 (AI Act) e la legge statale 132/2025.

L'architettura della legge

La proposta si articola su tre assi principali. Il primo è la governance: viene istituito un Comitato scientifico indipendente composto da cinque esperti, selezionati con procedura pubblica tra specialisti di discipline scientifiche, sociali e umanistiche, con funzioni consultive e propositive nei confronti della Giunta. Accanto ad esso, un Tavolo regionale che coinvolge università, IRCCS, organismi di ricerca, imprese, lavoratori ed enti locali, con riunioni minime tre volte l'anno.

Il secondo asse è la programmazione: la legge introduce un Programma strategico triennale per la ricerca, l'innovazione e l'AI, approvato dal Consiglio regionale, che definisce obiettivi, interventi e risorse. Tra le aree d'intervento esplicite figurano infrastrutture per ricerca e AI, open data, big data, brevetti, contrasto alla fuga di cervelli e trasferimento tecnologico. Il terzo asse riguarda due strumenti innovativi: la Piattaforma digitale per l'Innovazione, dotata di un milione di euro annui per il triennio 2026-2028, e la Carta regionale per lo sviluppo dell'intelligenza artificiale, documento programmatico che la Regione promuoverà presso imprese, università, enti di ricerca e organizzazioni della società civile.

I profili giuridici da tenere d'occhio

Dal punto di vista del diritto delle nuove tecnologie, la proposta lombarda merita attenzione su almeno tre fronti. Il primo riguarda il riparto di competenze costituzionali. La ricerca scientifica e tecnologica e il sostegno all'innovazione nei settori produttivi rientrano nella competenza concorrente Stato-Regioni ai sensi dell'art. 117, comma 3, della Costituzione. La legge lombarda si muove in questo perimetro, richiamando esplicitamente i principi del TUE e la normativa statale ed europea come limiti invalicabili. Alcune disposizioni - in particolare quelle che prevedono "norme tecniche su open data, big data e IA" nell'ambito del Programma strategico triennale - potrebbero tuttavia dar luogo a un dibattito interpretativo sui confini rispetto ad ambiti di competenza esclusiva statale. Si tratta di una questione aperta, su cui le opinioni tra i costituzionalisti non sono unanimi, e che l'iter consiliare potrà contribuire a chiarire. Il secondo profilo attiene al coordinamento con l'AI Act europeo. Il Regolamento (UE) 2024/1689 è direttamente applicabile in tutti gli Stati membri e non necessita di recepimento: le Regioni non possono né integrarlo né derogarlo. La legge lombarda si limita opportunamente a "promuovere, diffondere e monitorare" l'adozione dell'AI sul territorio, senza pretendere di disciplinare i requisiti tecnici dei sistemi.

Lombardia e Intelligenza Artificiale

Una legge regionale che guarda all'europa. I profili giuridici da tenere d'occhio

Questa scelta è giuridicamente corretta e coerente con il perimetro di azione che la normativa europea lascia agli enti territoriali. Il terzo profilo riguarda la Carta regionale per lo sviluppo dell'IA, strumento di soft law di sicuro interesse. Una Carta che orienta i firmatari verso un modello antropocentrico di AI, conforme alla normativa europea e alle migliori pratiche internazionali, non ha valore vincolante ma può produrre effetti concreti nella selezione dei fornitori tecnologici e nella valutazione degli investimenti pubblici e privati. È uno strumento già sperimentato in altri contesti europei e la sua efficacia dipenderà dalla qualità del documento che la Giunta produrrà e dalla capacità di costruire attorno ad esso una rete di adesioni significative.

Una legge che apre un cantiere

La proposta lombarda si distingue per l'approccio sistemico: non si limita a finanziare singoli progetti, ma tenta di costruire un'infrastruttura istituzionale stabile - governance, programmazione, partecipazione, monitoraggio - attorno ai temi dell'AI e dell'innovazione. In questo senso, il suo valore non si misura solo nei contenuti normativi ma nella visione che incorpora: quella di una regione che vuole essere protagonista attiva della transizione tecnologica, non semplice destinataria di indirizzi nazionali ed europei. L'iter consiliare sarà l'occasione per affinare il testo, precisare alcuni profili e consolidare la coerenza con il quadro normativo sovraordinato. Ma l'impostazione di fondo - costruire un sistema regionale della ricerca e dell'AI fondato su competenze, partecipazione e visione strategica di lungo periodo - è una direzione che vale la pena percorrere.

Allinea
Avvera Compliance Review
Marzo 2026

Caso Isybank

Il Garante sanzione per 17,6 milioni di euro

Con il provvedimento del 12 marzo 2026, il Garante per la protezione dei dati personali ha sanzionato Intesa Sanpaolo S.p.A. con una multa di 17.628.000 euro per violazione degli articoli 5, paragrafo 1, lettera a), 6, paragrafo 1, e 14 del GDPR. Al centro del caso l'operazione societaria con cui la Banca ha trasferito circa 2,4 milioni di clienti alla controllata Isybank S.p.A., banca digitale priva di sportelli fisici. Il provvedimento affronta questioni di rilievo generale - il confine tra perimetrazione aziendale e profilazione, i limiti del legittimo interesse, gli standard minimi di trasparenza - che vanno ben oltre il caso specifico e riguardano chiunque gestisca operazioni straordinarie coinvolgenti dati personali di larga scala.

La profilazione e la "perimetrazione"

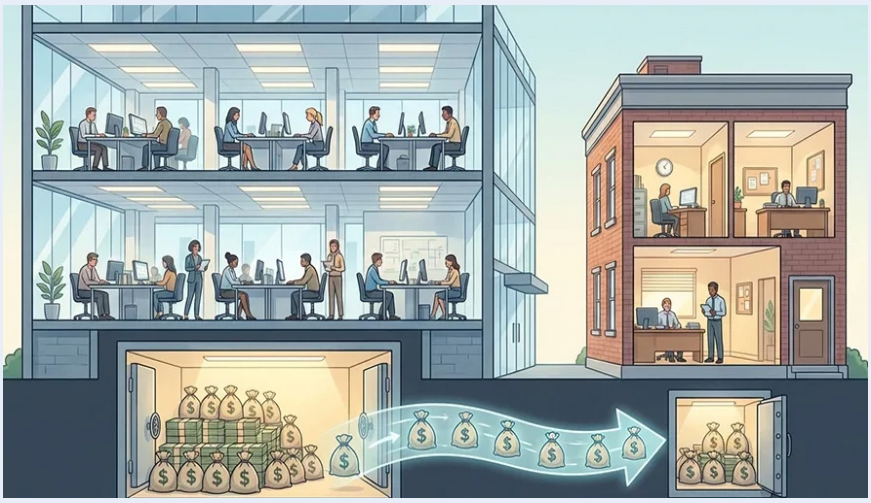
L'Autorità ha rilevato che le "progressive estrazioni dai sistemi gestionali" di Intesa Sanpaolo - attraverso cui sono stati selezionati i clienti in base a età, familiarità con i canali digitali, giacenze finanziarie inferiori a centomila euro e assenza di prodotti di investimento - integrano per loro stessa natura un trattamento automatizzato (anche se la Banca sostiene che non vi sia stato l'uso di strumenti automatizzati). Il coinvolgimento di gruppi di lavoro umani nella definizione dei criteri non esclude, a parere del Garante, l'automazione nell'esecuzione delle estrazioni. L'Autorità ha inoltre chiarito un principio di portata generale: la profilazione non richiede necessariamente una attività di marketing per essere tale. È profilazione qualsiasi trattamento automatizzato che valuti aspetti personali di una persona fisica per classificarla. La "propensione digitale" è esattamente uno di quegli aspetti. Il trattamento di profilazione è uno, ma le basi giuridiche devono essere distinte. Con riferimento al rapporto tra profilazione e comunicazione dei dati la Banca ha sostenuto che essa avesse quale base giuridica il legittimo interesse, applicabile alla comunicazione dei dati ai sensi dell'articolo 58 del Testo Unico Bancario.

Caso Isybank
Il Garante sanzione per 17,6 milioni di euro

La Banca ha ritenuto che questa base giuridica coprisse anche la fase di profilazione preliminare. L'Autorità ha operato su questo tema una distinzione netta, che costituisce il cuore del provvedimento: la profilazione è un trattamento autonomo, precedente e distinto rispetto alla comunicazione dei dati. Ciascun trattamento richiede una propria base giuridica, verificata separatamente. Il legittimo interesse invocato dalla Banca per la comunicazione non si estende automaticamente alla profilazione che la precede. Il Garante, verificato il Legitimate Interest Assessment prodotto dalla Banca, ha trova che riporta solo affermazioni tautologiche, prive di una reale ponderazione tra gli interessi del titolare e i diritti degli interessati. A proposito della valutazione del Garante pare essere inoltre elemento dirimente il fatto che solo 76.000 clienti (tra i 2,1 milioni di clienti individuati) hanno dato il consenso esplicito quando la campagna di contatto è stata effettuata su impulso dell'AGCM. Questo dato dimostra quanto le aspettative ragionevoli degli interessati fossero distanti dalle valutazioni della Banca.

Il silenzio-assenso nell'archivio dell'app
L'informativa relativa al trasferimento verso Isybank è stata inserita nella sezione archivio dell'area utente dell'app, senza notifica push, nel periodo estivo, confusa tra le notifiche ordinarie. Agli interessati è stato assegnato un termine per manifestare il dissenso: chi non ha risposto è stato considerato consenziente. Il Garante ha qualificato questo meccanismo come incompatibile con i principi di correttezza e trasparenza dell'articolo 5, paragrafo 1, lettera a), del GDPR, richiamando peraltro le stesse conclusioni cui era già giunto l'AGCM sul versante delle pratiche commerciali scorrette.

Le implicazioni pratiche
Il provvedimento consegna alle imprese almeno tre indicazioni operative.
Prima: ogni operazione di riorganizzazione societaria che richieda la selezione dei clienti sulla base di caratteristiche individuali è, in linea di principio, una profilazione e richiede una base giuridica specifica, distinta da quella applicabile al successivo trasferimento dei dati. Seconda: il Legitimate Interest Assessment deve essere un documento analitico e circostanziato, non una formula di stile. Terza: la trasparenza non si misura sull'esistenza formale dell'informativa, ma sulla sua effettiva accessibilità e comprensibilità nel contesto in cui viene resa.



Allinea
Avvera Compliance Review
Marzo 2026

IA generativa e diritto d'autore

La risoluzione del Parlamento Europeo apre un fronte che non chiuderà presto

Il 10 marzo 2026 il Parlamento europeo ha adottato con 460 voti a favore la risoluzione P10_TA(2026)0066 sul diritto d'autore e l'IA generativa. Non è ancora diritto vincolante - sarà la Commissione a decidere se avviare il processo legislativo - ma il segnale politico è netto e le implicazioni per chi opera nel mercato europeo sono già concrete.

Il nodo irrisolto: l'addestramento e gli usi successivi

I modelli di IA generativa sono addestrati su contenuti raccolti dalla rete che includono opere protette da copyright. Le eccezioni per il text and data mining previste dalla Direttiva (UE) 2019/790 non sono state pensate per coprire l'addestramento massivo di modelli commerciali su scala globale. La risoluzione lo riconosce esplicitamente: gli attuali meccanismi di opt-out sono poco pratici e mancano della trasparenza necessaria per un'attuazione efficace. Un elemento spesso trascurato è che la risoluzione estende gli obblighi anche agli utilizzi successivi all'addestramento: inferenza e generazione aumentata dal recupero (RAG), che avvengono in tempo reale. In questi casi, i crawler dovranno identificarsi presso gli operatori web e le imprese di IA dovranno conservare registri dettagliati delle loro attività di acquisizione dati. La trasparenza non si esaurisce al momento dell'addestramento.

"La risoluzione non risolve il problema. Lo formalizza"

I tre strumenti chiave

La risoluzione costruisce il proprio impianto su tre pilastri.

Il primo è la trasparenza obbligatoria: elenco dettagliato di tutti i contenuti protetti utilizzati, valido per qualsiasi provider che operi nel mercato UE indipendentemente da dove l'addestramento sia avvenuto. La risoluzione chiarisce che le informazioni sui contenuti di terzi non costituiscono segreto commerciale ai sensi del diritto UE: un argomento difensivo che molti provider avrebbero probabilmente tentato di usare.

Il secondo è la presunzione relativa: se il provider non rispetta gli obblighi di trasparenza, si presumerà che il modello abbia utilizzato opere protette senza autorizzazione. L'onere della prova si sposta sul provider, e in caso di soccombenza in giudizio le spese legali dei titolari dei diritti sono a suo carico.

Il terzo è il ruolo dell'EUIPO come intermediario istituzionale: gestione centralizzata dei registri di opt-out, supporto ai mercati delle licenze su base settoriale, istituzione di un Centro di conoscenze sul diritto d'autore. L'obiettivo è costruire infrastrutture che rendano praticabile la remunerazione equa senza bloccare l'innovazione.

Cosa fare adesso

Il contesto normativo si sta stringendo su più fronti simultaneamente: AI Act, GDPR, Code of Practice sull'etichettatura dei contenuti sintetici, e ora questa risoluzione. Per chi sviluppa o utilizza modelli generativi, quattro azioni sono non più differibili.

- Mappare la provenienza dei dati di addestramento e degli utilizzi successivi (inferenza, RAG), non solo la fase di training.
- Strutturare i meccanismi di opt-out in formati standardizzati e verificare che le esclusioni già espresse siano rispettate e documentate.
- Avviare negoziati in buona fede con i titolari dei diritti o le società di gestione collettiva per le categorie di contenuti più esposte.
- Integrare il controllo legale nella governance del ciclo di vita del modello, non come layer esterno ma come requisito di progettazione.

La risoluzione non risolve il problema. Lo formalizza. E nel diritto, formalizzare un problema è il primo passo verso la sua regolazione. Per chi opera in questo spazio, la domanda non è se adeguarsi: è con quanta anticipazione farlo rispetto alle norme che seguiranno.

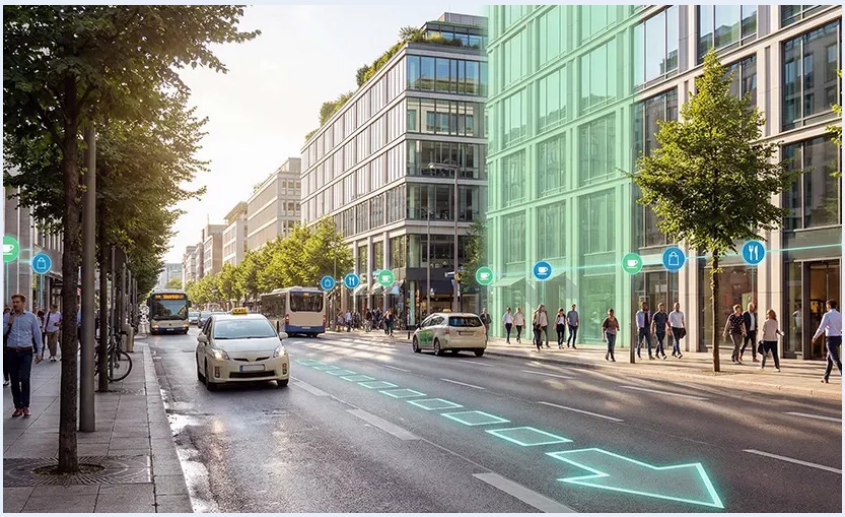
Allinea
Avvera Compliance Review
Marzo 2026

Ask Maps e Immersive Navigation

Quando la mappa diventa un assistente AI, cambiano anche le regole

Google integra Gemini in Maps e trasforma uno strumento di navigazione in una piattaforma conversazionale. Tre profili giuridici da tenere d'occhio: privacy, responsabilità per i contenuti generati dall'AI e obblighi da AI Act.

Google ha annunciato l'integrazione di Gemini in Google Maps attraverso due funzioni: Ask Maps, un'interfaccia conversazionale che risponde a domande complesse in linguaggio naturale attingendo all'archivio di luoghi, recensioni e dati degli utenti, e Immersive Navigation, che restituisce una rappresentazione tridimensionale del percorso combinando Street View e immagini aeree. Non si tratta di un aggiornamento estetico. È un cambio di paradigma: la mappa smette di essere uno strumento passivo e diventa un sistema che interpreta, suggerisce e raccomanda. E con questo passaggio emergono almeno tre profili giuridici che meritano attenzione.



1. Privacy e dati di localizzazione

Ask Maps funziona perché incrocia la richiesta dell'utente con un patrimonio di dati enorme: posizione in tempo reale, cronologia degli spostamenti, preferenze ricavate da ricerche precedenti, recensioni lasciate, foto caricate. Ogni domanda posta al sistema è anche un dato che alimenta il profilo dell'utente.

Dal punto di vista del GDPR, la domanda centrale è quale base giuridica regga questo trattamento. Il consenso, da solo, difficilmente è sufficiente per giustificare l'elaborazione continuativa di dati di localizzazione a fini di profilazione. Il legittimo interesse richiede un bilanciamento che tenga conto della ragionevole aspettativa dell'utente - e un sistema che ricorda dove sei stato, con chi e cosa hai cercato va ben oltre la navigazione. Le autorizzazioni da verificare, i diritti da esercitare e le informative da aggiornare non sono questioni teoriche: sono obblighi concreti per chiunque utilizzi le API di Maps in applicazioni rivolte a utenti europei.

"Il Digital Services Act impone obblighi di gestione dei contenuti illeciti alle piattaforme"

2. Responsabilità per i contenuti generati da Gemini

Quando Ask Maps suggerisce un ristorante, un posto di lavoro tranquillo o un itinerario, chi risponde se il suggerimento è sbagliato, fuorviante o causa un danno? La risposta non è semplice. Gemini genera raccomandazioni a partire da dati aggregati - recensioni, foto, informazioni sui luoghi - ma l'output è presentato come una risposta affidabile a una domanda specifica. Il Digital Services Act impone obblighi di gestione dei contenuti illeciti alle piattaforme, ma il perimetro diventa più complesso quando il contenuto è generato dalla piattaforma stessa, non solo ospitato. Se un sistema AI raccomanda un luogo che si rivela pericoloso o un'attività che non esiste più, la responsabilità di Google come provider del modello è diversa da quella di una piattaforma che si limita a indicizzare contenuti di terzi. È un confine che la giurisprudenza europea non ha ancora tracciato con precisione, ma che i prossimi anni metteranno alla prova.

Ask Maps e Immersive Navigation
Quando la mappa diventa un assistente AI, cambiano anche le regole

3. AI Act e sistemi di raccomandazione
Ask Maps è un sistema di raccomandazione basato su AI. La classificazione rilevante ai fini dell'AI Act dipende dal contesto d'uso: un sistema che influenza le scelte di mobilità, consumo e fruizione dello spazio urbano di milioni di persone non è neutro. L'AI Act non lo classifica automaticamente come sistema ad alto rischio, ma impone comunque, per i modelli di uso generale come Gemini, obblighi di trasparenza, documentazione tecnica e gestione del rischio sistemico.
Per i deployer che integrano le API di Maps nelle proprie applicazioni, il quadro è ancora più articolato: il deployer assume obblighi propri rispetto all'uso specifico che fa del sistema, indipendentemente da ciò che Google garantisce a livello di provider. La compliance non si esaurisce nell'accettare i termini di servizio.

Conclusione
Google Maps con Gemini è un prodotto tecnologicamente sofisticato. Dal punto di vista giuridico, è anche un caso di studio in tempo reale su come i sistemi AI conversazionali si inseriscano in ecosistemi digitali già regolati - e su quante domande aperte restino ancora senza risposta.

Allinea
Avvera Compliance Review
Marzo 2026

AI ACT Omnibus
Il Consiglio UE apre il cantiere della semplificazione

Il 13 marzo 2026 il Consiglio dell'Unione Europea ha adottato la propria posizione negoziale sulla proposta di modifica dell'AI Act, nell'ambito del pacchetto legislativo "Omnibus" dell'agenda di semplificazione europea. Non si tratta di un testo definitivo - la posizione del Consiglio costituisce il mandato per avviare i negoziati interistituzionali in trilogo con il Parlamento europeo e la Commissione - ma segna un passaggio politico rilevante: per la prima volta dall'entrata in vigore del Regolamento (UE) 2024/1689, le istituzioni europee aprono formalmente il cantiere della sua revisione.

Il contesto: perché si modifica un regolamento appena entrato in vigore
L'AI Act è in vigore dal 1° agosto 2024, ma la sua applicazione è scaglionata nel tempo. La scadenza critica è il 2 agosto 2026, data in cui gli obblighi per i sistemi AI ad alto rischio dovrebbero entrare in vigore. Il problema è che gli strumenti tecnici necessari - standard armonizzati, specifiche comuni, linee guida operative - non sono ancora disponibili. Imporre alle imprese il rispetto di regole senza fornire i riferimenti tecnici per farlo sarebbe un paradosso normativo. Da qui la proposta di semplificazione.

"Imporre alle imprese il rispetto di regole senza fornire i riferimenti tecnici per farlo sarebbe un paradosso normativo"

Le modifiche principali
Il cuore della proposta riguarda le tempistiche. La Commissione aveva proposto un ritardo di 16 mesi, subordinato alla conferma della disponibilità degli standard tecnici. Il Consiglio ha tradotto questo principio in date fisse: i sistemi autonomi sarebbero soggetti alle nuove norme dal 2 dicembre 2027, mentre i sistemi embedded - integrati in prodotti regolamentati - dal 2 agosto 2028.
Sul fronte delle esenzioni, la proposta estende alle imprese di medie dimensioni (small mid-caps) le esenzioni già previste per le PMI, amplia la possibilità di trattare dati personali sensibili per la rilevazione dei bias e rafforza i poteri dell'AI Office riducendo la frammentazione nella governance. Sul piano delle nuove tutele, viene introdotto un esplicito divieto per i sistemi AI di generare contenuti intimi non consensuali, incluso materiale che coinvolge minori. Un'aggiunta che dimostra come il processo di revisione non sia orientato esclusivamente alla deregolamentazione.

AI Act Omnibus
Il Consiglio UE apre il cantiere della semplificazione

Cosa resta invariato
Prima di trarre conclusioni affrettate, è necessario ricordare che il testo definitivo non è ancora concordato e le date riviste restano soggette a modifica nel trilogo. Soprattutto, l'AI Act nella sua versione attuale rimane pienamente operativo. Gli obblighi già in vigore - AI literacy dal 2 febbraio 2025, modelli general-purpose dal 2 agosto 2025, trasparenza per i sistemi generativi dal 2 agosto 2026 - non sono toccati dalla proposta di semplificazione.

Conclusioni
La posizione del Consiglio è un segnale importante: il legislatore europeo ha preso atto che la complessità tecnica del Regolamento richiede più tempo per essere attuata in modo coerente. Ma sarebbe un errore leggere questa apertura come un allentamento della pressione regolatoria. Le date vengono spostate, non cancellate. Gli obblighi vengono calibrati, non eliminati. E nel frattempo il trilogo - con il Parlamento europeo storicamente più rigoroso del Consiglio su questi temi - potrebbe ancora spostare gli equilibri in direzioni non scontate.
Il calendario è stretto: il voto del Parlamento europeo è previsto per giugno, la pubblicazione degli emendamenti per luglio 2026. Per le imprese che attendono il testo definitivo prima di adeguarsi, il rischio di trovarsi in ritardo è concreto. Chi ha già avviato un percorso strutturato di compliance guadagnerà tempo e flessibilità, qualunque sia la data finale che il trilogo stabilirà. Chi aspetta rischia di ritrovarsi, come già accaduto con il GDPR, a inseguire una scadenza con le risorse esaurite.

Allinea

Avvera Compliance Review

Newsletter Informativa
riservata a clienti e partner
di Avvera

Marzo

AVVERA | SB Società Benefit

Largo Umberto Boccioni 1
21040 Origgio VA
T. +39 02 96515401

Altre sedi
Milano - Pesaro - Udine

avvera.it - info@avvera.it