**INNOVA JUS**
*Rivista mensile del Centro Studi Innova Jus*

Anno I · Numero 1
Maggio 2026

NUMERO MONOGRAFICO · ATTUALITÀ NORMATIVA EUROPEA

# IL DIGITAL OMNIBUS

## *La riconfigurazione del diritto digitale europeo*

- L’accordo politico del 7 maggio 2026 sul Digital Omnibus on AI
- Le modifiche al GDPR: dato personale, violazioni, DPIA
- Cookie banner ed ePrivacy: la fine della consent fatigue?
- Lo «Stop the Clock» dell’AI Act: nuove scadenze
- Le posizioni critiche di EDPB ed EDPS
- Profili operativi per il DPO e per la pubblica amministrazione

**CENTRO STUDI INNOVA JUS**
Direttore scientifico: Prof. Avv. Michele Iaselli
innovajus.it

# INNOVA JUS

*Rivista mensile del Centro Studi Innova Jus*

***Anno I · Numero 1 · Maggio 2026***

**Testata**
Innova Jus. Rivista mensile del Centro Studi Innova Jus.

**Direzione scientifica**
Prof. Avv. Michele Iaselli — Direttore del Centro Studi Innova Jus, docente di Informatica giuridica e Diritto dell'intelligenza artificiale presso LUISS Guido Carli e Università di Cassino, Coordinatore del Comitato Scientifico di Federprivacy.

**Tema del numero**
Il Digital Omnibus. La riconfigurazione del diritto digitale europeo.

**Periodicità**
Mensile. Ogni numero è dedicato a un argomento monografico di diritto dell'innovazione, con approfondimenti sistematici, ricognizione delle fonti primarie e profili operativi.

**Editore**
Centro Studi Innova Jus — Via Giovanni Merliani, 19 — 80127 Napoli (Italia). Sito: innovajus.it — Posta elettronica: info@innovajus.it

**Lingua**
Italiano.

**Supporto e diffusione**
Edizione elettronica in formato PDF, diffusa gratuitamente sul sito dell'editore.

**Avvertenza metodologica**
Tutti i riferimenti normativi, gli atti istituzionali e le date richiamati nei contributi sono stati verificati su fonti ufficiali primarie (Commissione europea, Parlamento europeo, Consiglio dell'Unione europea, EDPB, EDPS, Gazzetta Ufficiale dell'Unione europea). Eventuali profili in evoluzione sono espressamente segnalati come tali. Il fascicolo è chiuso alla data del 10 maggio 2026.

# Sommario

EDITORIALE

# Un omnibus per l’Europa digitale

*di Michele Iaselli*

*Il diritto digitale europeo, costruito a strati successivi nell’arco dell’ultimo decennio, ha raggiunto una soglia di complessità tale da generare ciò che la Commissione, mutuando il lessico del rapporto Draghi del 2024, definisce apertamente un «innovation gap». Il Digital Omnibus presentato il 19 novembre 2025 risponde a questa diagnosi con un’operazione di tecnica normativa inusuale per dimensione e ambizione: un intervento orizzontale che attraversa GDPR, AI Act, NIS2, Data Act, DORA, ePrivacy e Data Governance Act, riscrivendone in modo mirato passaggi cruciali per l’applicazione pratica.*

La domanda che ogni operatore del diritto si è posta in questi mesi non è se l’Omnibus rappresenti una semplificazione, ma se la sua semplificazione erodi il livello di tutela. È la stessa domanda, nei suoi termini sostanziali, sollevata dalle autorità di controllo nelle Joint Opinions 1/2026 e 2/2026 di EDPB ed EDPS, adottate rispettivamente il 20 gennaio (sul Digital Omnibus on AI) e l’11 febbraio 2026 (sul Digital Omnibus generale), ed è la domanda che attraversa il dibattito parlamentare e quello dottrinale fino all’accordo politico provvisorio raggiunto nelle prime ore del 7 maggio 2026 sul Digital Omnibus on AI. Quel mattino, dopo il fallimento del trilogo del 28 aprile, i co-legislatori hanno trovato un’intesa che riscrive le scadenze applicative dei sistemi di intelligenza artificiale ad alto rischio: il 2 agosto 2026 cessa di essere il muro applicativo che era stato fissato dal Regolamento (UE) 2024/1689 ed entrano nel calendario europeo le nuove date del 2 dicembre 2027 e del 2 agosto 2028.

Si tratta di uno spostamento delle lancette, non di una loro disattivazione. È un punto sul quale converrà tornare più volte nel corso di questo numero, perché segna la differenza tra una proroga di natura tecnica, motivata dalla maturazione delle norme armonizzate e dei meccanismi di valutazione della conformità, e una rinegoziazione politica dell’architettura di tutela. La distinzione è tutt’altro che accademica: chi opera sul fronte della compliance sa che l’orizzonte di pianificazione è cambiato, ma sa anche che la struttura risk-based del Regolamento è rimasta intatta e che gli obblighi sostanziali sui sistemi ad alto rischio non sono stati indeboliti.

Il fascicolo che il lettore ha tra le mani è il numero d’esordio della rivista del Centro Studi Innova Jus. Abbiamo scelto di inaugurarlo con un tema che è al tempo stesso d’attualità stretta e di portata sistematica perché ci sembra fedele alla vocazione del Centro: monitorare il cambiamento normativo nel momento in cui si compie, ricondurlo a un disegno coerente, restituirlo all’operatore in forma utilizzabile. La cadenza sarà mensile e ogni numero sarà dedicato a una questione monografica. La regola che ci siamo dati è una sola, ma inderogabile: ogni dato, ogni citazione, ogni riferimento normativo passa per la verifica diretta sulla fonte primaria. È una fatica che il lettore non vedrà, ma che spiega perché in queste pagine non si troverà mai un «sembra che» travestito da affermazione perentoria.

Nei sei contributi che seguono — cronaca dell’accordo, modifiche al GDPR, riforma del consenso ePrivacy, slittamento dell’AI Act, posizioni critiche delle autorità di controllo, profili operativi per il DPO e per la pubblica amministrazione — abbiamo cercato di tenere insieme due esigenze: la precisione tecnica dei rinvii normativi e una scrittura discorsiva che restituisca la posta in gioco. Chiude il fascicolo una nota prospettica sul Digital Fitness Check, la seconda fase di semplificazione che la Commissione ha già annunciato per il primo trimestre del 2027 e che, in qualche misura, dirà quanto del modello costruito tra il 2016 e il 2024 il legislatore

europeo intenderà conservare.

Resta una considerazione di metodo. Il Digital Omnibus è un atto di governo del cambiamento, non un punto di arrivo. Per chi fa diritto della tecnologia, accettare che la materia di studio sia in movimento permanente è una premessa ovvia; organizzare il lavoro intellettuale in modo da seguirla senza inseguirla è una sfida concreta. Questa rivista nasce con l'ambizione di accompagnare quel movimento, mese per mese.

CRONACA NORMATIVA

# L’accordo politico del 7 maggio 2026

*Anatomia di una trattativa che sembrava chiusa e si è riaperta*

*Nelle prime ore di giovedì 7 maggio 2026, dopo dodici ore di negoziato e a nove giorni di distanza dal fallimento del trilogo del 28 aprile, i co-legislatori europei hanno raggiunto un accordo politico provvisorio sul Digital Omnibus on AI. La notizia è stata diffusa attraverso i comunicati ufficiali del Parlamento europeo e del Consiglio dell’Unione europea ed è stata oggetto di una conferenza stampa congiunta tenuta a Strasburgo dai correlatori Arba Kokalari (PPE, Svezia) per la commissione IMCO e Michael McNamara (Renew, Irlanda) per la commissione LIBE.*

La cronaca è in sé istruttiva. Il percorso istituzionale era stato compresso al massimo: posizione del Consiglio adottata il 13 marzo 2026 (comunicato 189/26), relazione congiunta IMCO/LIBE A10-0073/2026 il 18 marzo, voto della plenaria del Parlamento europeo il 26 marzo 2026 con 569 voti favorevoli, 45 contrari e 23 astensioni, primo trilogo politico immediatamente successivo, secondo trilogo concluso senza accordo il 28 aprile per il dissenso sull’architettura della valutazione di conformità dei sistemi di intelligenza artificiale incorporati nei prodotti di cui all’Allegato I dell’AI Act. La conferenza stampa prevista per il giorno successivo era stata annullata, e diverse fonti istituzionali e professionali indicavano nel 13 maggio la finestra utile successiva. La chiusura del file in data 7 maggio rappresenta dunque un evento politicamente significativo prima ancora che giuridicamente rilevante.

Il contenuto sostanziale dell’intesa è ricostruibile in modo affidabile, ancor prima che il testo consolidato sia disponibile, sulla base dei comunicati ufficiali e delle ricostruzioni offerte dagli studi specializzati che hanno seguito il dossier. Tre i pilastri dell’accordo. Il primo riguarda lo slittamento dell’applicazione degli obblighi sui sistemi ad alto rischio: per le sezioni da 1 a 3 del capo III del Regolamento (UE) 2024/1689 le scadenze diventano il 2 dicembre 2027 per i sistemi di cui all’Allegato III (biometria, infrastrutture critiche, lavoro, istruzione, forze dell’ordine, giustizia, migrazione, servizi essenziali) e il 2 agosto 2028 per i sistemi che costituiscono componenti di sicurezza dei prodotti regolati dall’Allegato I (ascensori, giocattoli, dispositivi medici, macchinari). Si tratta di scadenze fisse, non condizionate alla pubblicazione delle norme armonizzate, a differenza del meccanismo «stop the clock» originariamente proposto dalla Commissione.

Il secondo pilastro è il restringimento del periodo transitorio per gli obblighi di marcatura dei contenuti generati artificialmente di cui all’articolo 50, paragrafo 2, dell’AI Act. La data applicativa generale resta il 2 agosto 2026, ma i fornitori di sistemi già immessi sul mercato prima di quella data dovranno conformarsi entro il 2 dicembre 2026: una finestra di tre mesi più stretta rispetto al 2 febbraio 2027 inizialmente proposto dalla Commissione e sostenuto in prima battuta dal Consiglio. Per i fornitori di sistemi generativi di immagini, video e audio già in commercio, questa diventa la scadenza operativa più prossima e concretamente impegnativa che emerge dall’accordo.

Il terzo pilastro è di natura prescrittiva piuttosto che differente: l’introduzione di una nuova fattispecie di pratica vietata all’articolo 5 dell’AI Act. Saranno proibiti i sistemi di intelligenza artificiale che generano materiale pedopornografico (CSAM) o che creano immagini, video o tracce audio raffiguranti le parti intime di una persona identificabile in modo non consensuale — le cosiddette applicazioni «nudifier». Il divieto, che dovrà essere recepito nei sistemi entro il 2 dicembre 2026, non investe soltanto le applicazioni concepite a tale scopo ma anche i fornitori di modelli generativi di carattere generale che non implementino misure ragionevoli

di salvaguardia contro questo tipo di abuso.

Restano da indicare alcuni elementi minori ma non irrilevanti. Le agevolazioni già previste per le piccole e medie imprese sono estese alle small mid-cap (fino a 750 dipendenti e 150 milioni di euro di fatturato), istituendo così una nuova categoria rilevante anche ai fini del calcolo delle sanzioni. Viene reintrodotto, sebbene fosse stato eliminato dalla proposta originaria, l'obbligo di registrazione nella banca dati europea per i sistemi che il fornitore ritiene non ad alto rischio sulla base dell'autovalutazione prevista dall'articolo 6, paragrafo 3. Si rafforza, infine, la posizione dell'AI Office in chiave di vigilanza coordinata sui sistemi basati su modelli di carattere generale e su quelli incorporati nelle piattaforme online di grandi dimensioni.

Sul piano operativo il messaggio è nitido. L'accordo richiede ancora il voto formale di Parlamento e Consiglio e la revisione giuridico-linguistica prima della pubblicazione in Gazzetta Ufficiale: entrambe le istituzioni hanno dichiarato l'intenzione di completare l'adozione prima del 2 agosto 2026. Fino a quel momento, e con prudenza professionale, i programmi di adeguamento non vanno arrestati: il muro del 2 agosto resta giuridicamente vigente fino all'entrata in vigore dell'Omnibus, e le nuove scadenze potranno essere assunte come baseline di pianificazione solo dopo la formalizzazione dell'atto.

GDPR

# Definizione di dato personale, violazioni, DPIA

*Le modifiche più incisive al regolamento generale sulla protezione dei dati*

*Il Digital Omnibus generale (COM(2025) 837) interviene sul GDPR su tre fronti che meritano una trattazione distinta perché toccano altrettanti snodi della compliance quotidiana: la definizione di dato personale, il regime delle violazioni e la valutazione d'impatto. È utile premettere che si tratta di emendamenti mirati, non di una riscrittura del Regolamento (UE) 2016/679. La Commissione qualifica esplicitamente l'operazione come «adeguamento, chiarimento e semplificazione delle disposizioni del GDPR, senza incidere sui principi fondamentali».*

La modifica più controversa investe l'articolo 4, punto 1, del GDPR, e precisamente la nozione di dato personale. La proposta della Commissione introduce un elemento di relatività entity-based: un'informazione è personale per un titolare se questi dispone di mezzi ragionevolmente utilizzabili per identificare la persona fisica cui essa si riferisce. La stessa informazione, in capo a un soggetto diverso che non disponga di tali mezzi, può non costituire dato personale. L'obiettivo dichiarato è codificare l'orientamento della Corte di giustizia emerso nei casi Breyer (C-582/14) e SRB (T-557/20, oggi confermato in appello), e fornire una base esplicita al regime della pseudonimizzazione: se la re-identificazione risulta praticamente impossibile per l'entità ricevente sulla base della tecnologia disponibile, il dato pseudonimizzato può cadere fuori dal perimetro di applicazione del GDPR per quel ricevente e per quegli specifici scopi.

EDPB ed EDPS, nella Joint Opinion 2/2026 dell'11 febbraio 2026, hanno espresso forti riserve. Le autorità hanno chiesto ai co-legislatori di non adottare la proposta nella sua formulazione attuale, sostenendo che l'intervento eccede i confini di un emendamento tecnico, va oltre la giurisprudenza della Corte di giustizia e rischia di restringere significativamente il concetto stesso di dato personale. Particolare contrarietà ha suscitato la previsione che la Commissione possa adottare atti di esecuzione per stabilire i criteri tecnici della pseudonimizzazione, una soluzione che — nelle parole delle autorità — sottrarrebbe al co-legislatore una decisione che incide direttamente sull'ambito di applicazione del diritto europeo della protezione dei dati. I testi di compromesso circolati in sede di Consiglio lasciano presagire che la disposizione possa essere sostanzialmente rivista o eliminata nel testo finale, ma il negoziato resta aperto.

La seconda area di intervento riguarda il regime delle violazioni di cui agli articoli 33 e 34 del GDPR. La proposta agisce su tre leve. In primo luogo, allinea la soglia di notificazione all'autorità di controllo a quella prevista per la comunicazione all'interessato: solo le violazioni che presentano un rischio elevato per i diritti e le libertà delle persone fisiche dovranno essere notificate, abbandonando la doppia soglia attualmente vigente. In secondo luogo, estende il termine di notifica da settantadue a novantasei ore dal momento della conoscenza, consentendo al titolare un margine più ampio per la triage forense e la qualificazione del rischio. In terzo luogo, istituisce uno sportello unico di notifica gestito dall'ENISA, che fungerebbe da punto di accesso comune anche per le notifiche dovute ai sensi della direttiva NIS2, del regolamento DORA, della direttiva CER e del regolamento eIDAS, secondo il principio del «report once, use many times».

L'innalzamento della soglia richiede un'avvertenza. Il passaggio da «rischio» a «alto rischio» come criterio di notifica non comporta una mera diminuzione del numero di segnalazioni: ridistribuisce l'onere valutativo a carico del titolare, che dovrà documentare con maggior rigore le ragioni per cui una violazione è stata classificata come non ad alto rischio. La pratica ricorrente di ransomware risolto con ripristino da backup, oggi

normalmente notificato al Garante e non comunicato all'interessato, non rientrerebbe più, in linea di massima, nell'obbligo di segnalazione: una semplificazione apprezzabile dal punto di vista operativo, ma che presuppone metodologie interne di valutazione del rischio robuste, aggiornate e auditabili. Spetterà all'EDPB, secondo la proposta, predisporre un modello unificato di notifica e una lista delle circostanze in cui una violazione è verosimilmente ad alto rischio, da rivedersi almeno ogni tre anni.

La terza area attiene all'articolo 35 del GDPR e alla valutazione d'impatto sulla protezione dei dati. Anche qui l'intervento punta all'armonizzazione: l'EDPB redigerebbe liste europee uniformi delle attività di trattamento che richiedono la DPIA e di quelle che non la richiedono, oltre a un modello standard di metodologia e contenuto. Le liste nazionali, una volta approvate quelle europee con atto di esecuzione della Commissione, sarebbero superate; nel periodo intermedio resterebbero in vigore. Per l'Italia significa convivenza temporanea tra il provvedimento del Garante dell'11 ottobre 2018 (allegato 1) e le future indicazioni europee, e progressivo allineamento dei criteri operativi, con quanto ne deriva in termini di aggiornamento dei registri delle attività e dei modelli interni.

Restano da menzionare due interventi minori ma operativamente significativi. L'articolo 12, paragrafo 5, viene modificato per consentire al titolare di rifiutare la richiesta di accesso o di richiedere un onorario ragionevole quando l'interessato esercita il diritto per finalità diverse dalla protezione dei propri dati personali, una previsione che si presta a impieghi delicati nel contenzioso civile e che le autorità di controllo hanno chiesto di chiarire. L'articolo 9 viene integrato con una nuova base di legittimità per il trattamento di dati appartenenti a categorie particolari, ai fini della rilevazione e correzione di bias nei sistemi di intelligenza artificiale, e con un richiamo esplicito alla possibilità di fondare il trattamento per l'addestramento dei modelli sul legittimo interesse, fatta salva la verifica di necessità e proporzionalità e la conduzione del balancing test.

Il bilancio complessivo, alla luce delle modifiche al GDPR, è ambivalente. La parte sulle violazioni e sulla DPIA realizza una semplificazione ragionevole, corregge sovrapposizioni con NIS2 e DORA, e introduce strumenti di armonizzazione utili. La parte sulla definizione di dato personale apre una questione politica e sistematica che il dibattito interistituzionale dovrà risolvere senza scorciatoie tecniche. Il rischio, segnalato da più voci dottrinali, è che una nozione cardine del diritto europeo della protezione dei dati venga ridefinita di fatto attraverso la regolamentazione attuativa, anziché attraverso il passaggio legislativo che una scelta di tale rilievo richiederebbe.

ePRIVACY

# Cookie banner: la fine della consent fatigue?

*Articoli 88a e 88b GDPR: nuova architettura del consenso sui dispositivi terminali*

*Il fascicolo del Digital Omnibus che con maggior probabilità finirà sotto gli occhi del cittadino europeo non riguarda l'intelligenza artificiale e nemmeno la definizione di dato personale: riguarda il banner dei cookie. La Commissione propone di trasferire all'interno del GDPR la disciplina del consenso al trattamento di informazioni memorizzate o accessibili sull'apparecchiatura terminale dell'utente, oggi dettata dall'articolo 5, paragrafo 3, della direttiva ePrivacy 2002/58/CE, attraverso due nuovi articoli — 88a e 88b — che ridefiniscono in profondità il governo del consenso sui dispositivi.*

Il problema cui la proposta intende rispondere è noto a chiunque navighi in rete: la cosiddetta consent fatigue. La proliferazione dei pop-up, il loro frequente ricorso a dark patterns che inducono all'accettazione, la mancanza di standardizzazione tra siti hanno trasformato un istituto pensato come strumento di tutela in una pratica generalmente subita o aggirata. Le indagini delle autorità nazionali e gli studi commissionati dalla stessa Commissione hanno documentato non solo il fastidio soggettivo dell'utente, ma anche un effettivo svuotamento della funzione informativa del consenso.

L'architettura proposta poggia su quattro pilastri. Il primo è l'individuazione di un perimetro di attività esenti da consenso, ulteriore rispetto a quelle già previste dall'ePrivacy: oltre alla strict necessity per il servizio richiesto dall'utente, si aggiungono in particolare la misurazione di pubblico aggregata condotta dal solo titolare del sito (cosiddetta first-party analytics) e la gestione tecnica della sicurezza, secondo soglie e modalità da specificarsi. La logica è chiara: limitare il consenso a ciò che effettivamente comporta una scelta significativa per l'utente, sgombrando il campo dalle ipotesi a basso impatto.

Il secondo pilastro è il principio del rifiuto a un click. L'interfaccia di raccolta del consenso dovrà consentire il diniego con la stessa facilità dell'accettazione: un pulsante di pari prominenza grafica, accessibile senza percorsi di scoraggiamento, senza opzioni intermedie più invasive presentate per difetto. È la formalizzazione, in chiave normativa, di un orientamento già consolidato presso il Comitato europeo e presso il Garante italiano, ma che numerose pratiche di mercato continuavano a disattendere.

Il terzo pilastro è il moratorium di sei mesi: una volta che l'utente abbia rifiutato il consenso per una determinata finalità, il medesimo consenso non può essere richiesto nuovamente per almeno sei mesi. Si tratta di una previsione che, pur nella sua semplicità, modifica strutturalmente l'economia del web tracking: i siti non potranno più ripresentare il banner a ogni visita o a ogni cambio di dispositivo nella speranza di ottenere un'accettazione che non era stata concessa la prima volta. Resta da vedere come la regola interagirà con la gestione tecnica dei cookie ricordando le preferenze stesse, dato che la persistenza del rifiuto presuppone una qualche forma di memoria.

Il quarto pilastro è forse il più ambizioso: l'introduzione di segnali automatizzati e leggibili dalla macchina, attraverso i quali l'utente esprime preferenze a livello di browser o di sistema operativo, vincolando il sito a rispettarle senza ulteriore interrogazione. Il modello richiama il Global Privacy Control statunitense e le iniziative europee di standardizzazione del Do Not Track. I browser non qualificati come PMI saranno tenuti a fornire i mezzi tecnici necessari. La transizione verso un sistema di consenso espresso a livello di browser è il

vero salto di paradigma della proposta: se attuata in modo coordinato, sposterebbe il centro di gravità del consenso dal singolo sito alla configurazione personale dell'utente, con effetti dirompenti sull'industria pubblicitaria digitale.

Una nota tecnica merita attenzione. La proposta prevede l'allineamento delle sanzioni per le violazioni delle norme sui cookie a quelle generali del GDPR — fino a venti milioni di euro o al quattro per cento del fatturato mondiale annuo — superando la frammentazione attuale, in cui ogni Stato membro applica plafond sanzionatori differenti. Per l'Italia, dove il Garante ha già esercitato un'attività sanzionatoria robusta sulla base del Codice della privacy, la novità è meno traumatica che per altri ordinamenti, ma uniforma il rischio europeo per gli operatori multinazionali.

Le criticità non mancano. EDPB ed EDPS hanno sostenuto l'obiettivo di contrastare la consent fatigue ma hanno chiesto chiarimenti sul perimetro delle nuove esenzioni, in particolare sulla first-party analytics, per evitare che essa finisca per coprire pratiche di profilazione che giustificherebbero il consenso. Una parte della dottrina osserva inoltre che la traslazione dei cookie dalla direttiva ePrivacy al GDPR — pur giustificabile sul piano della razionalizzazione — rischia di lasciare irrisolta la questione di fondo: la proposta di un nuovo regolamento ePrivacy giace in stallo da anni, e la scelta di intervenire con tecnica omnibus sul GDPR potrebbe consolidare di fatto un regime ibrido, con la direttiva ePrivacy svuotata nei suoi profili più incisivi ma formalmente in vigore.

Per l'operatore, il messaggio operativo è chiaro. La revisione completa dei banner, ampiamente fatta o rifatta nel 2023 e nel 2024 sulla scorta delle linee guida del Garante, dovrà probabilmente essere ripensata di nuovo, con un'attenzione particolare al pulsante di rifiuto, alla tracciabilità della scelta e all'adozione progressiva dei segnali automatizzati. Si tratta di un investimento che si aggiungerà, nel breve, ai costi di compliance, ma che dovrebbe ridurli strutturalmente nel medio periodo.

AI ACT

# Lo «Stop the Clock» sui sistemi ad alto rischio

*Le nuove scadenze del 2 dicembre 2027 e del 2 agosto 2028*

*Lo slittamento dell'applicazione degli obblighi sui sistemi di intelligenza artificiale ad alto rischio è il provvedimento di maggiore impatto pratico contenuto nel Digital Omnibus. La proposta originaria della Commissione, presentata il 19 novembre 2025, prevedeva un meccanismo flessibile, denominato «stop the clock», in base al quale l'applicazione delle regole sarebbe stata sospesa fino alla pubblicazione delle norme armonizzate, delle specifiche tecniche comuni e degli orientamenti necessari alla compliance. L'accordo politico del 7 maggio 2026 ha trasformato quel meccanismo flessibile in due scadenze fisse e inderogabili.*

La ragione della proroga è nota. Le comunicazioni provenienti dal CEN-CENELEC Joint Technical Committee 21, l'organismo cui è affidata la redazione delle norme armonizzate a supporto dell'AI Act, indicavano che il pacchetto completo non sarebbe stato disponibile prima di dicembre 2026. Le imprese, dal canto loro, segnalavano in modo unanime di aver bisogno di almeno dodici mesi per costruire la conformità a una singola norma armonizzata, figurarsi al pacchetto completo dei requisiti tecnici previsti per i sistemi ad alto rischio. La data del 2 agosto 2026, inizialmente fissata dal Regolamento (UE) 2024/1689, era diventata progressivamente irrealistica, e il rischio era una applicazione formale delle regole non accompagnata dagli strumenti che ne consentono il rispetto sostanziale.

Le nuove date di applicazione, come anticipato, sono il 2 dicembre 2027 per i sistemi di cui all'Allegato III dell'AI Act — quelli stand-alone in settori sensibili come biometria, infrastrutture critiche, formazione, lavoro, giustizia, forze dell'ordine, migrazione e servizi essenziali — e il 2 agosto 2028 per i sistemi che costituiscono componenti di sicurezza dei prodotti regolati dall'Allegato I, ossia macchinari, ascensori, dispositivi medici, giocattoli, apparecchiature radio. Si tratta, rispettivamente, di una proroga di sedici e di dodici mesi rispetto alle scadenze originarie. È utile sottolineare che la struttura risk-based del Regolamento non è stata toccata: il sistema di classificazione, gli obblighi sostanziali in capo a fornitori e deployer, l'architettura della valutazione di conformità restano quelli del 2024.

Un punto delicato dell'accordo riguarda i sistemi dell'Allegato I, che era stato l'elemento di rottura del trilogo del 28 aprile. La soluzione di compromesso prevede che i prodotti regolati dalle normative settoriali di sicurezza non debbano rispettare cumulativamente le regole settoriali e quelle dell'AI Act: la disciplina di settore prevale, a condizione che la Commissione adotti, attraverso atti di esecuzione, le misure necessarie a garantire un livello equivalente di tutela della salute e della sicurezza. Per il regolamento macchine, in particolare, l'AI Act verrebbe disapplicato come fonte diretta, e i requisiti specifici per i sistemi di intelligenza artificiale sarebbero introdotti attraverso atti delegati adottati sulla base del regolamento macchine stesso. Si tratta di una soluzione che evita duplicazioni ma che presuppone una capacità normativa attuativa del legislatore europeo nei prossimi diciotto mesi non scontata.

L'articolo 50 dell'AI Act, che disciplina le obbligazioni di trasparenza per i sistemi che interagiscono con le persone fisiche e per i sistemi che generano contenuti, segue una traiettoria leggermente diversa. La data generale di applicazione resta il 2 agosto 2026. Il paragrafo 2, relativo all'obbligo di marcatura dei contenuti audio, video, immagini e testo prodotti artificialmente in formato leggibile dalla macchina, beneficia di un periodo transitorio per i sistemi già immessi sul mercato prima della data di applicazione: questi fornitori

dovranno conformarsi entro il 2 dicembre 2026. Si tratta della scadenza più prossima e più stringente dell'intero pacchetto, e impone ai fornitori di sistemi generativi già attivi di implementare, in circa sette mesi dall'accordo, strumenti di watermarking effettivi, robusti rispetto a manipolazioni ragionevoli e interoperabili a livello di lettura automatica.

Restano da segnalare alcuni interventi laterali. Le disposizioni sulla literacy in materia di intelligenza artificiale di cui all'articolo 4 vengono riformulate: l'obbligo a carico di fornitori e deployer di garantire un livello sufficiente di preparazione del personale viene mantenuto per i sistemi ad alto rischio, mentre per gli altri sistemi viene tradotto in un dovere generale di promozione a carico della Commissione e degli Stati membri. Una scelta che la dottrina ha criticato osservando che il problema dello shadow AI nelle organizzazioni è reale e crescente, e che la responsabilità dei vertici aziendali per la governance degli strumenti effettivamente utilizzati dai dipendenti rimane comunque ferma, anche al di là delle previsioni dell'AI Act.

Il quadro che ne emerge è quello di un legislatore che sceglie il pragmatismo rispetto al rigore formale. Lo slittamento non significa abbandono, ma le imprese che avevano interrotto i programmi di adeguamento confidando in ulteriori rinvii sono avvertite: l'accordo del 7 maggio è quasi certamente l'ultima proroga di natura politica, e i tempi diventano da ora in avanti tecnici. Chi avesse pianificato sulla scadenza di agosto 2026 dispone di un orizzonte ampliato, ma l'orizzonte resta finito: il 2 dicembre 2027 dista, alla data di chiusura di questo numero, meno di venti mesi.

TUTELE

# Le posizioni critiche di EDPB ed EDPS

*La Joint Opinion 2/2026 e i timori di un arretramento delle garanzie*

*L'11 febbraio 2026 il Comitato europeo per la protezione dei dati e il Garante europeo della protezione dei dati hanno adottato la Joint Opinion 2/2026 sulla proposta di Digital Omnibus generale, dopo che il 20 gennaio 2026 le stesse autorità avevano già reso pubblica la Joint Opinion 1/2026 sul Digital Omnibus on AI. Il documento dell'11 febbraio merita lettura integrale: è metodologicamente sobrio, tecnicamente dettagliato, e politicamente franco. Le autorità condividono l'obiettivo della semplificazione e della competitività, sollevano però obiezioni precise su un numero limitato ma significativo di profili.*

L'obiezione più articolata, come già evidenziato nel contributo dedicato alle modifiche al GDPR, riguarda la definizione di dato personale. EDPB ed EDPS sostengono che la formulazione proposta dalla Commissione eccede i confini di un emendamento mirato e tecnico. Il rilievo non è di stile: secondo le autorità, la proposta non riflette accuratamente l'orientamento della Corte di giustizia, ma ne offre una versione che ne amplifica gli effetti deflattivi del perimetro di tutela. La nozione di dato personale, ricordano le autorità, è il presupposto applicativo dell'intero diritto europeo della protezione dei dati: una sua restrizione, anche tecnicamente fondata, ridisegna il campo di intervento del GDPR. Per questa ragione, le autorità chiedono che ogni eventuale chiarimento definitorio sia compiuto direttamente dal co-legislatore e non delegato alla Commissione attraverso atti di esecuzione, soprattutto quando si tratta di stabilire i criteri tecnici della pseudonimizzazione.

Una seconda area di preoccupazione riguarda l'articolo 12, paragrafo 5, e la nuova facoltà di rifiutare la richiesta di accesso quando l'interessato la eserciti per finalità diverse dalla protezione dei propri dati. Le autorità condividono l'obiettivo di consentire al titolare di reagire ad abusi del diritto, ma osservano che la finalità perseguita dall'interessato non può essere il criterio per qualificare un comportamento come abusivo. Il diritto di accesso ha una finalità funzionale — consentire all'interessato di verificare la liceità del trattamento — ma non può essere strumentalmente legato alla manifestazione di un'intenzione protettiva. La proposta, nella sua attuale formulazione, rischia di consentire al titolare valutazioni discrezionali su un piano che le autorità ritengono debba restare oggettivo: l'abuso, se sussiste, è nelle modalità di esercizio del diritto, non nelle finalità che vi sono sottese.

Sul fronte del processo decisionale automatizzato, EDPB ed EDPS hanno chiesto chiarimenti significativi. Le modifiche all'articolo 22 del GDPR — che disciplina il diritto a non essere sottoposti a decisioni basate unicamente sul trattamento automatizzato — sono presentate dalla Commissione come tecniche, ma toccano un punto di intersezione delicato con l'AI Act. Le autorità chiedono che le modifiche siano riformulate in modo da rendere chiaro il loro effetto giuridico e da coordinarle con l'articolo 14 dell'AI Act in materia di sorveglianza umana. Diversamente, il rischio è che la disciplina dell'articolo 22, già oggi non sempre ben coordinata con la nuova architettura europea dell'intelligenza artificiale, perda ulteriormente di efficacia operativa.

Sul versante del consenso ai cookie, le autorità si sono dichiarate favorevoli all'obiettivo di riduzione della consent fatigue, ma hanno suggerito chiarimenti sul perimetro delle nuove esenzioni. La preoccupazione, come anticipato, riguarda in particolare la categoria della first-party analytics: senza una definizione rigorosa, l'esenzione potrebbe coprire pratiche che presentano profili di profilazione individuale e che, per coerenza con la giurisprudenza europea, dovrebbero restare soggette al consenso. Le autorità hanno inoltre sottolineato

l’importanza che il sistema dei segnali automatizzati di cui al nuovo articolo 88b sia progettato in modo da non riprodurre, a livello di browser, i dark patterns che la riforma intende eliminare a livello di sito.

Una valutazione complessiva: la Joint Opinion 1/2026 è un documento di mediazione, non di rottura. EDPB ed EDPS non chiedono il ritiro della proposta, ma il suo emendamento puntuale. La forza della loro posizione sta nella scelta di concentrare le riserve su un nucleo limitato di disposizioni, lasciando salvi gli aspetti di semplificazione che le autorità condividono. È una postura che assegna ai co-legislatori una responsabilità chiara: se le proposte più controverse passano nella loro formulazione attuale, il responsabile politico non potrà sostenere di non essere stato avvertito.

A questa posizione istituzionale si è aggiunta, l’8 aprile 2026, una lettera aperta firmata da BEUC e da oltre cento organizzazioni della società civile, centrata sulla preservazione dell’integrità dell’AI Act e sul rifiuto di qualsiasi riapertura del compromesso politico raggiunto nel 2024. Il dibattito pubblico ha così accompagnato il dibattito istituzionale, restituendo al Digital Omnibus la dimensione di una scelta politica e non puramente tecnica.

Il testo finale dovrà misurarsi con queste critiche. È ragionevole attendersi che alcuni profili più sensibili — la definizione di dato personale, la delega alla Commissione su pseudonimizzazione, il criterio della finalità nell’accesso — vengano riformulati. Quanto, e con quale soglia di tutela effettiva, resterà della proposta originaria, sarà il vero indicatore della tenuta dell’architettura europea della protezione dei dati nei prossimi anni.

PROFILI OPERATIVI

# Cosa cambia per il DPO e per la pubblica amministrazione

*Indicazioni di lavoro per chi gestisce la conformità*

*Le modifiche introdotte dal Digital Omnibus, anche solo nella loro versione attualmente negoziata, richiedono al Data Protection Officer e alle strutture di compliance della pubblica amministrazione una rilettura sistematica delle politiche, delle procedure e degli strumenti operativi. Non si tratta di un esercizio di adeguamento puntuale: sono in gioco le procedure di notifica, i processi di DPIA, i contratti con i fornitori di sistemi di intelligenza artificiale, le clausole di accettazione dei cookie e le politiche sulla literacy in materia di IA.*

Il primo cantiere riguarda la procedura di notifica delle violazioni. Il passaggio dalla soglia del «rischio» a quella dell'«alto rischio» e l'estensione del termine a novantasei ore impongono una rivisitazione delle procedure interne di valutazione e classificazione. Il rischio operativo — che il DPO deve gestire con particolare attenzione — è quello di classificare come «non ad alto rischio» violazioni che l'autorità di controllo qualificherebbe diversamente. La risposta non può essere prudenziale al punto da svuotare la semplificazione, ma deve poggiare su metodologie di risk assessment robuste, tracciabili, periodicamente aggiornate. È prevedibile che gli ordini professionali e le associazioni di categoria predispongano modelli di riferimento; sarà in ogni caso opportuno attendere il modello unificato che l'EDPB è chiamato a redigere prima di procedere a riforme strutturali.

Per la pubblica amministrazione italiana, e in particolare per i comuni che utilizzano sistematicamente l'articolo 33 del GDPR, il punto critico riguarda l'interfaccia con la NIS2. La direttiva, recepita in Italia con il decreto legislativo 4 settembre 2024, n. 138, prevede notifiche di incidenti a CSIRT-Italia secondo un calendario distinto da quello del GDPR. Lo sportello unico previsto dal Digital Omnibus — una volta operativo, il che richiederà tempo — consentirebbe di assolvere a entrambe le notifiche con un unico invio. Nel frattempo, le procedure interne devono continuare a contemplare le doppie notifiche, ma vale la pena predisporle in modo modulare, così da consentire una migrazione fluida quando la single-entry point sarà attiva.

Il secondo cantiere riguarda la valutazione d'impatto. Le liste europee uniformi che dovrebbero essere predisposte dall'EDPB sostituiranno, una volta approvate, le liste nazionali. Per i titolari italiani, il riferimento attuale resta il provvedimento del Garante dell'11 ottobre 2018 e i suoi aggiornamenti successivi. È ragionevole continuare a operare sulla base di quel quadro fino alla pubblicazione delle liste europee, ma è utile, già oggi, costruire i registri delle DPIA in formato strutturato e standardizzato, che ne consenta una rapida mappatura sulle nuove liste comuni quando saranno disponibili.

Il terzo cantiere riguarda il consenso. Il banner attualmente in uso, anche se recentemente conformato alle linee guida del Garante, andrà quasi certamente rivisto: il pulsante di rifiuto a un click, il moratorium di sei mesi e la progressiva accettazione dei segnali automatizzati richiedono interventi tecnici sull'infrastruttura del sito. Per le amministrazioni pubbliche, il tema è meno critico (i siti istituzionali tipicamente non utilizzano cookie di profilazione), ma resta da considerare la posizione delle municipalizzate e degli enti che gestiscono servizi al pubblico in forma commerciale, per i quali l'adeguamento dovrà essere strutturale.

Il quarto cantiere, quello più strategico, riguarda l'AI Act. Lo slittamento al 2 dicembre 2027 e al 2 agosto 2028 restituisce un orizzonte di pianificazione che molti consideravano già saltato. Le amministrazioni che avevano avviato la mappatura dei sistemi di intelligenza artificiale di cui all'Allegato III — in particolare quelli utilizzati per la valutazione dei dipendenti, per il rilascio di prestazioni essenziali, per l'accesso a servizi pubblici — possono completare il lavoro con un margine più ragionevole. Quelle che lo avevano rinviato non possono più farlo: l'orizzonte di venti mesi non lascia spazio per un approccio reattivo.

Una considerazione specifica merita la legge 23 settembre 2025, n. 132, recante disposizioni e deleghe in materia di intelligenza artificiale, la cui applicazione si svilupperà nei prossimi mesi attraverso i decreti legislativi delegati. Il coordinamento tra il quadro nazionale italiano e l'AI Act, già oggi delicato, verrà ulteriormente complicato dalle modifiche introdotte dal Digital Omnibus. I decreti legislativi attuativi della legge 132/2025, attesi nei prossimi mesi, dovranno tener conto del nuovo calendario europeo e, presumibilmente, delle modifiche al regime sanzionatorio e a quello della valutazione di conformità. Per il DPO che opera nell'amministrazione pubblica, il monitoraggio congiunto dei due binari — europeo e nazionale — è da considerarsi un'attività ordinaria nei prossimi diciotto mesi.

Restano due ambiti che meritano vigilanza, anche se non sono al centro del Digital Omnibus. Il primo è quello dei contratti con i fornitori di sistemi di intelligenza artificiale, che dovranno essere riletti per verificare la coerenza con le nuove definizioni di small mid-cap, con la diversa allocazione delle responsabilità tra fornitore e deployer e con il nuovo regime di marcatura per i sistemi generativi. Il secondo è quello della formazione del personale: anche con le modifiche all'articolo 4 dell'AI Act, l'obbligo sostanziale di garantire un livello adeguato di literacy resta confermato per i sistemi ad alto rischio, e in ogni caso costituisce una misura di buona governance dell'organizzazione.

In sintesi: il Digital Omnibus non disinnesca, ridistribuisce. La compliance non diminuisce, cambia forma. Per chi gestisce la protezione dei dati e la conformità all'AI Act in un'organizzazione pubblica o privata, i prossimi diciotto mesi saranno tra i più densi dall'entrata in vigore del GDPR.

PROSPETTIVE

# Verso il Digital Fitness Check

*La seconda fase della semplificazione del rulebook digitale*

*Il Digital Omnibus è esplicitamente presentato dalla Commissione come la prima fase di un'operazione più ampia di razionalizzazione del diritto digitale europeo. La seconda fase prende il nome di Digital Fitness Check ed è stata avviata con una call for evidence e una consultazione pubblica aperte dal 19 novembre 2025 all'11 marzo 2026. L'adozione formale dei risultati è prevista per il primo trimestre del 2027.*

Mentre il Digital Omnibus è un atto normativo che modifica disposizioni in vigore, il Digital Fitness Check è una valutazione di sistema. Il suo obiettivo dichiarato è studiare l'interazione tra le diverse fonti del rulebook digitale e il loro impatto cumulativo sulle imprese, individuando aggiustamenti più strutturali di quelli compatibili con un intervento omnibus mirato. È prevedibile che dal Fitness Check emergano proposte di carattere sistematico: una possibile fusione di più atti, l'abrogazione di disposizioni rese ridondanti dall'evoluzione normativa, la riallocazione di competenze tra le autorità europee e nazionali.

La direzione è in parte già visibile. Il Digital Omnibus contiene esso stesso embrioni di razionalizzazione strutturale: la fusione delle disposizioni del Data Governance Act, della direttiva sull'Open Data e del regolamento sulla libera circolazione dei dati non personali in un Data Act ristrutturato; l'abrogazione della Platform-to-Business Regulation, le cui previsioni sono in larga misura assorbite dal Digital Services Act. Sono mosse che lasciano intravedere un disegno più ampio, in cui il diritto digitale europeo si organizza per blocchi tematici coerenti anziché per stratificazioni successive.

Tre questioni saranno verosimilmente al centro del Fitness Check. La prima è il rapporto tra le autorità di vigilanza. Oggi un'impresa che opera nel mercato digitale europeo si interfaccia con i Garanti nazionali per la protezione dei dati, con le autorità nazionali competenti per la NIS2, con i Digital Services Coordinator, con le autorità di vigilanza della concorrenza per il DMA, con le autorità nazionali competenti per l'AI Act, oltre che con la Commissione e l'AI Office a livello europeo. La frammentazione è fonte di costi diretti e di incoerenze applicative. Una rilettura coordinata delle competenze è attesa.

La seconda questione è quella dei rapporti con il diritto della concorrenza e con la disciplina settoriale. Più di una norma del diritto digitale — si pensi alle disposizioni sui mercati digitali, sulla portabilità dei dati, sull'obbligo di interoperabilità — opera in un'area di sovrapposizione con il diritto antitrust, con la disciplina dei servizi finanziari, con la regolamentazione sanitaria. Il Fitness Check potrà chiarire quale fonte prevale nei casi di concorso, e attraverso quali strumenti di coordinamento.

La terza questione è forse la più sensibile: la sostenibilità del modello europeo di regolazione digitale rispetto alle dinamiche globali. Il Brussels Effect, ossia la capacità del diritto europeo di esercitare un'influenza extraterritoriale attraverso la dimensione del proprio mercato, ha funzionato pienamente per il GDPR ed è stato in parte all'opera per l'AI Act. Ma il consenso politico per regolazioni rigorose è oggi più fragile di quanto fosse nel 2016, e la pressione competitiva proveniente da modelli regolatori meno invasivi — segnatamente quelli statunitense e britannico — si è fatta più esplicita. Il Fitness Check non potrà evitare di affrontare la questione: si tratterà di stabilire fino a che punto la semplificazione può spingersi senza snaturare il modello europeo costruito a partire dalla Carta dei diritti fondamentali e dall'articolo 16 del Trattato sul funzionamento

dell’Unione.

Per i lettori di questa rivista, il Fitness Check sarà oggetto di un numero monografico nei prossimi mesi. Per ora ci limitiamo a segnalarlo come la cornice politica entro cui collocare il Digital Omnibus: non un episodio isolato di adeguamento, ma il primo passo di una strategia di rilettura complessiva del rulebook digitale che si sviluppa lungo la legislatura 2024-2029 della Commissione von der Leyen II e che, presumibilmente, arriverà a maturazione tra il 2027 e il 2028.

RIFERIMENTI

# Indicazioni bibliografiche e fonti primarie

*Atti istituzionali, opinioni e materiali consultati*

## Fonti normative

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), in GUUE L 119 del 4.5.2016.

Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale), in GUUE L del 12.7.2024.

Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (direttiva NIS2).

Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche).

Legge 23 settembre 2025, n. 132, recante disposizioni e deleghe al Governo in materia di intelligenza artificiale.

## Atti istituzionali e documenti di consultazione

Commissione europea, COM(2025) 837 final, Proposta di regolamento del Parlamento europeo e del Consiglio relativo alla semplificazione del quadro normativo digitale (Digital Omnibus), 19 novembre 2025.

Commissione europea, COM(2025) 836 final, Proposta di regolamento del Parlamento europeo e del Consiglio relativo alla semplificazione dell'attuazione delle norme armonizzate in materia di intelligenza artificiale (Digital Omnibus on AI), 19 novembre 2025.

Consiglio dell'Unione europea, comunicato stampa 189/26, Council agrees position to streamline rules on artificial intelligence, 13 marzo 2026.

Parlamento europeo, voto della plenaria sul Digital Omnibus on AI, 26 marzo 2026 (569 voti favorevoli, 45 contrari, 23 astensioni).

Parlamento europeo, comunicato stampa AI Act: deal on simplification measures, ban on "nudifier" apps, 7 maggio 2026.

Consiglio dell'Unione europea, Artificial intelligence: Council and Parliament agree to simplify and streamline rules, comunicato stampa del 7 maggio 2026.

Commissione europea, comunicato stampa EU agrees to simplify AI rules to boost innovation and ban "nudification" apps to protect citizens, 7 maggio 2026.

EDPB-EDPS, Joint Opinion 1/2026 on the Proposal for a Regulation as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), 20 gennaio 2026.

EDPB-EDPS, Joint Opinion 2/2026 sulla proposta di regolamento di semplificazione del quadro normativo digitale (Digital Omnibus generale), 11 febbraio 2026.

Banca centrale europea, parere sulla proposta di regolamento di semplificazione del quadro normativo digitale, 10 marzo 2026.

Commissione europea, Digital Fitness Check, call for evidence e consultazione pubblica, 19 novembre 2025 - 11 marzo 2026.

Camera dei Deputati, XIV Commissione (Politiche dell'Unione europea), documento sulle osservazioni al pacchetto Digital Omnibus, 24 febbraio 2026.

## Giurisprudenza richiamata

Corte di giustizia dell'Unione europea, sentenza del 19 ottobre 2016, Patrick Breyer c. Repubblica federale di Germania, causa C-582/14, ECLI:EU:C:2016:779.

Tribunale dell'Unione europea, sentenza del 26 aprile 2023, Single Resolution Board (SRB) c. EDPS, causa T-557/20, ECLI:EU:T:2023:219, e successivi sviluppi in sede di impugnazione.

## Letteratura tecnica e analisi specialistiche

Per la ricostruzione delle posizioni negoziali e per il dettaglio delle modifiche puntuali sono stati consultati, fra gli altri, i materiali di analisi pubblicati nel periodo dicembre 2025 – maggio 2026 da Sidley Austin LLP, White & Case LLP, Bird & Bird, Morrison & Foerster, Loyens & Loeff, Hunton Andrews Kurth, Slaughter and May, Maples Group, Matheson, Timelex, IAPP. Le ricostruzioni sono state in ogni caso verificate sui comunicati ufficiali e sui testi pubblicati dalle istituzioni europee.

---

**Avvertenza finale.** Il presente fascicolo è chiuso alla data del 10 maggio 2026. Il testo consolidato dell'accordo del 7 maggio sul Digital Omnibus on AI sarà disponibile nelle settimane successive alla conferenza stampa di Strasburgo e potrà contenere precisazioni che incidono su singoli profili qui trattati. La rivista darà conto delle eventuali modifiche significative nei prossimi numeri.

---

**INNOVA JUS** — Rivista del Centro Studi · Anno I · Numero 1 · Maggio 2026 · Tema monografico: il Digital Omnibus. · Direzione scientifica: Prof. Avv. Michele Iaselli. · innovajus.it