DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

APPROFONDIMENTI

Digital Omnibus e AI Act: verso un sistema di governance integrato

La semplificazione come stress test della governance digitale per banche e assicurazioni

Giugno 2026

Alessandro Ferrari, Partner, Head of Technology Sector, DLA Piper

Alessandro Ferrari, Partner, Head of Technology Sector, DLA Piper

Alessandro Ferrari

Alessandro Ferrari è Partner del dipartimento Intellectual Property & Technology e dirige il Sector Technology in Italia e si occupa principalmente di diritto applicato alla tecnologia, assistendo i clienti in questioni transactional, advisory and IT litigation. Ha esperienza nella redazione e negoziazione di accordi strategici e cross-border di outsourcing di processi aziendali e di altri contratti commerciali, IT e relativi alla proprietà intellettuale in diversi settori e in diverse geografie. Ha inoltre esperienza nella consulenza su tutti gli aspetti del processo di sourcing/approvvigionamento, compreso lo sviluppo della struttura dell'accordo, la negoziazione e l'assistenza ai clienti nell'implementazione e nelle strategie di integrazione, nella governance e nei performance management regimes.

Studio Legale Tributario Associato

DLA Piper

1. Sommario

Il Digital Omnibus non dovrebbe essere letto dagli intermediari finanziari e assicurativi come una semplice proroga degli obblighi dell'AI Act. Il rinvio di alcune scadenze, la razionalizzazione degli adempimenti e il tentativo di coordinamento con altri regimi europei sono piuttosto l'occasione per trasformare la compliance AI da esercizio documentale a sistema di governance integrato con DORA, GDPR, outsourcing, product governance, model risk management e presidi di condotta verso clienti e assicurati.

Per banche, intermediari e compagnie assicurative, il punto centrale non è attendere la data finale di applicazione, ma decidere ora quali sistemi AI mappare, quali classificare come high-risk, quali assoggettare a controlli rafforzati anche se non formalmente high-risk, e come contrattualizzare il ricorso a modelli general-purpose e soluzioni agentiche.

Il Digital Omnibus sull'AI Act non è ancora, al momento, una disciplina definitivamente consolidata: Consiglio e Parlamento hanno raggiunto un accordo provvisorio, destinato a essere formalmente adottato e pubblicato prima di produrre effetti vincolanti. Tuttavia, il testo concordato è ormai sufficientemente maturo per essere utilizzato come baseline di pianificazione interna. Per banche, intermediari e imprese assicurative, la domanda non è quindi se attendere, ma come utilizzare il tempo aggiuntivo per rendere governabili i sistemi AI già in uso o in fase di procurement.

2. La semplificazione non è una sospensione della compliance

Il Digital Omnibus nasce con una finalità dichiarata di semplificazione. La Commissione europea ha presentato il pacchetto il 19 novembre 2025 per introdurre misure mirate volte a rendere l'attuazione dell'AI Act più fluida, proporzionata e coerente con la disponibilità di standard, strumenti di supporto e infrastrutture di governance. Il 7 maggio 2026 Consiglio e Parlamento europeo hanno raggiunto un accordo provvisorio sulla componente AI del pacchetto, parte dell'Omnibus VII, con l'obiettivo di semplificare il quadro digitale e l'implementazione dell'AI Act.

Il dato più rilevante per gli operatori è il rinvio degli obblighi relativi a molti sistemi AI high-risk: per i sistemi di cui all'Allegato III, la nuova data indicata è il 2 dicembre 2027; per i sistemi high-risk incorpo-

vedi l'articolo online

rati in prodotti o componenti di sicurezza di cui all'Allegato I, la data indicata è il 2 agosto 2028. Restano tuttavia ferme altre componenti del regime, inclusi alcuni obblighi di trasparenza e il nuovo divieto relativo a sistemi AI destinati a generare contenuti di abuso sessuale su minori o immagini intime non consensuali.

Il rinvio riguarda soprattutto gli obblighi high-risk di Chapter III, Sections 1-3. Non tutti gli obblighi dell'AI Act vengono spostati: i divieti e l'AI literacy sono già applicabili dal 2 febbraio 2025; il Capo V sui modelli GPAI ha avviato il proprio percorso applicativo dal 2 agosto 2025, con regimi transitori per i modelli già immessi sul mercato; e le regole di trasparenza ex articolo 50 restano in larga parte agganciate al 2 agosto 2026, con una finestra specifica fino al 2 dicembre 2026 per il marking ex articolo 50(2) di taluni sistemi già immessi sul mercato.

Questa scansione temporale va maneggiata con cautela. L'accordo è ancora provvisorio e le modifiche produrranno effetti solo dopo adozione formale e pubblicazione nella Gazzetta ufficiale dell'Unione europea. Ne deriva un primo suggerimento operativo: gli intermediari non dovrebbero costruire i piani di compliance su un'aspettativa di rinvio "in bianco", ma su una doppia traiettoria, distinguendo tra obblighi già applicabili, obblighi probabilmente rinviati e obblighi che restano incerti sino alla chiusura dell'iter legislativo.

In altri termini, il Digital Omnibus non autorizza a fermare i cantieri AI. Al contrario, rende meno difendibile l'approccio attendista: se il legislatore concede più tempo proprio perché gli standard e gli strumenti applicativi non sono ancora pienamente maturi, le imprese vigilate dovrebbero usare quel tempo per costruire inventari, classificazioni, controlli, contratti e flussi di escalation.

3. Perché il tema è particolarmente rilevante per istituzioni finanziarie e assicurative

L'AI Act ha una portata orizzontale, ma il settore finanziario e assicurativo è tra quelli in cui l'intersezione con regole esistenti è più intensa. La ragione è duplice.

Da un lato, banche, intermediari e assicurazioni utilizzano già modelli predittivi, sistemi di scoring, strumenti antifrode, motori di pricing, sistemi di customer interaction, soluzioni di KYC, AML, gestione sinistri, reclami e monitoraggio dei rischi. Dall'altro lato, questi usi incidono spesso sull'accesso a servizi essenziali, sulla posizione economica del cliente, sull'assicurabilità, sul premio, sul merito creditizio o sull'esperienza contrattuale del consumatore.

L'AI Act, nella sua impostazione originaria, mira a creare un mercato interno dell'AI affidabile, promuovendo l'innovazione ma garantendo un elevato livello di protezione di salute, sicurezza e diritti fondamentali. Il regolamento è complementare rispetto ad altre discipline UE, inclusi protezione dati, tutela dei consumatori, sicurezza dei prodotti, diritti fondamentali e rimedi risarcitori. Questa complementarità è centrale per gli intermediari vigilati: la compliance AI non sostituisce GDPR, DORA, CRR, Solvency II, IDD, PSD, AML o regole di condotta, ma si innesta su tali framework.

La stessa EBA ha evidenziato che i requisiti dell'AI Act per sistemi high-risk utilizzati nella valutazione del merito creditizio e nel credit scoring sono sostanzialmente complementari rispetto alla normativa bancaria e sui pagamenti, e che l'assenza di contraddizioni significative non elimina la necessità di integrare i presidi AI nei framework esistenti. In ambito assicurativo, EIOPA ha ricordato che i sistemi AI per risk assessment e pricing in life e health insurance sono considerati high-risk e ha pubblicato un'Opinion sull'AI governance per chiarire l'applicazione dei principi Solvency II e IDD all'uso dell'AI nel settore assicurativo.

La conseguenza pratica è che l'AI Act non introduce un "nuovo silos" regolamentare. Per le istituzioni finanziarie e assicurative, il tema è come innestare l'AI governance in controlli già maturi: risk management, compliance, internal audit, outsourcing, ICT risk, data governance, model validation, product approval process, gestione reclami, incident reporting e presidi di trasparenza verso la clientela.

Questo è anche il punto che rende il Digital Omnibus particolarmente interessante per banche e assicurazioni: la semplificazione orizzontale del quadro digitale deve essere tradotta in una governance settoriale, coerente con la vigilanza prudenziale, la vigilanza di condotta e la resilienza operativa digitale.

4. Il vero primo adempimento: un inventario AI che serva alla governance, non solo alla classificazione

Molti programmi AI Act partono da una domanda apparentemente semplice: "quali sistemi sono high-risk?". È una domanda necessaria, ma non sufficiente. Prima ancora occorre sapere quali sistemi AI

l'ente utilizza, sviluppa, acquista, integra o modifica; per quale finalità; con quali dati; con quale livello di autonomia; con quale impatto sul cliente; con quale ruolo giuridico dell'ente nella catena del valore.

Le draft guidelines sulla classificazione high-risk ricordano che non ogni software o sistema automatizzato è un sistema AI: occorre verificare la definizione dell'articolo 3(1) e, poi, la riconducibilità ai due scenari dell'articolo 6, cioè sistemi incorporati in prodotti o componenti di sicurezza soggetti a valutazione di conformità di terza parte, oppure casi d'uso elencati nell'Allegato III. Le linee guida sull'Allegato III sottolineano inoltre che l'elenco dei casi high-risk è esaustivo e che la classificazione dipende dall'intended purpose, non dall'etichetta commerciale del prodotto o dal grado di intervento umano.

Per un intermediario, l'inventario dovrebbe quindi contenere almeno: descrizione del caso d'uso; business owner; fornitore; modello sottostante; dati utilizzati; output prodotti; destinatari dell'output; decisioni supportate; presenza di dati personali o categorie particolari; customer impact; ruolo dell'ente come provider o deployer; eventuale uso di GPAI; eventuale integrazione con processi DORA-critical; valutazione preliminare AI Act; valutazione GDPR; eventuale outsourcing o ICT third-party risk.

L'inventario deve anche distinguere tra AI "visibile" e AI "incorporata". La prima comprende chatbot, assistenti documentali, strumenti di generazione contenuti, sistemi di supporto al relationship manager o al liquidatore sinistri. La seconda include AI inserita in piattaforme vendor, sistemi antifrode, strumenti CRM, motori di pricing, software di underwriting, soluzioni HR, monitoraggio transazionale, cyber detection e sistemi di workflow automation. Il rischio maggiore, nella pratica, è che la seconda categoria resti fuori dal perimetro perché non acquistata come "AI tool", ma come componente di una suite gestionale.

Per questo l'inventario AI dovrebbe essere costruito come un registro di governance e non come una mera survey legale: dovrebbe consentire al board e alle funzioni di controllo di sapere quali decisioni sono influenzate da sistemi AI, quali fornitori sono critici, quali dati alimentano i modelli, quali controlli umani sono effettivi e quali sistemi potrebbero generare obblighi paralleli ai sensi di AI Act, GDPR, DORA o normativa settoriale.

5. High-risk nel credito e nell'assicurazione: tracciare bene i confini

Per banche e intermediari, il caso più evidente è quello dei sistemi AI destinati a valutare la creditworthiness di persone fisiche o a stabilirne il credit score, con esclusione dei sistemi utilizzati per finalità di rilevazione delle frodi finanziarie. Per le assicurazioni, il caso centrale è quello dei sistemi destinati al risk assessment e al pricing in relazione a persone fisiche nel ramo vita e salute.

È quindi essenziale chiarire che l'high-risk non riguarda ogni modello bancario, prudenziale o assicurativo. Riguarda, in particolare, la valutazione della creditworthiness o del credit score di persone fisiche e il risk assessment/pricing in life and health insurance rispetto a persone fisiche. Non ogni modello di portafoglio, antifrode, AML, prudenziale, pricing commerciale o claims management è automaticamente high-risk ai sensi dell'Allegato III.

Qui il contributo operativo delle draft guidelines sull'Allegato III è particolarmente utile. Non tutti gli strumenti che si collocano nel ciclo del credito o dell'assicurazione rientrano automaticamente nei casi high-risk. Ad esempio, sistemi di customer support che aiutano il richiedente a comprendere o compilare una domanda di credito, senza partecipare alla valutazione formale del merito creditizio, possono restare fuori dal punto 5(b). Lo stesso può valere per sistemi di gestione reclami successivi alla decisione, per il monitoraggio interno dell'esposizione creditizia a fini prudenziali, per la valutazione del collateral come asset, o per talune forme di margin credit su servizi privati non essenziali. Nel settore assicurativo, sistemi di product design o claims management possono essere distinti dal risk assessment e pricing individuale vita/salute, se non determinano l'assicurabilità o il premio del singolo.

Questa distinzione non va però trasformata in un arbitraggio formale. Il punto decisivo è la funzione effettiva del sistema nel processo decisionale. Un tool presentato come "supporto commerciale" ma utilizzato di fatto per filtrare clienti, raccomandare condizioni peggiorative, generare soglie di accettazione o incidere sul prezzo individuale può assumere rilevanza high-risk. Il suggerimento pratico è predisporre per ogni sistema una scheda di boundary assessment: dove inizia e finisce il sistema AI; quali input riceve; quali output produce; chi li usa; se l'output è vincolante o solo informativo; quali decisioni a valle dipendono dall'output; quali controlli umani sono effettivi.

Particolarmente delicato è il rapporto tra sistemi prudenziali e sistemi di credit scoring. Le draft gui-

vedi l'articolo online

delines chiariscono che un sistema usato esclusivamente per calcolare esposizioni ponderate per il rischio nell'ambito IRB o per finalità prudenziali non è high-risk solo perché rilevante ai fini CRR o Solvency II, se non è destinato a valutare il merito creditizio della persona fisica o a stabilirne il credit score. Tuttavia, se un sistema prudenziale alimenta o viene alimentato da un sistema di scoring, occorre una valutazione caso per caso dei confini tra i sistemi.

Questo è un punto essenziale per banche e assicurazioni: il perimetro AI Act non coincide sempre con il perimetro model risk o prudenziale, ma i due perimetri si parlano. Occorre evitare sia l'errore di attrarre nell'AI Act qualunque modello regolamentare interno, sia l'errore opposto di escludere sistemi che incidono sulla posizione del cliente solo perché nati in ambito risk management.

6. Il periodo di rinvio come test di governance: ownership, AI literacy e ruolo delle autorità settoriali

Il Digital Omnibus sposta in avanti parte degli obblighi high-risk, ma non sposta in avanti la necessità di decidere chi governa l'AI all'interno dell'intermediario. Per banche e assicurazioni, il tempo aggiuntivo ha valore solo se viene trasformato in un programma di governance: identificazione dei responsabili, classificazione dei casi d'uso, integrazione con DORA e outsourcing, presidio dei fornitori, formazione del personale e reporting verso gli organi aziendali. In questo senso, il tema organizzativo non è esterno al Digital Omnibus, ma ne è la conseguenza pratica più immediata.

Le FAQ della Commissione chiariscono che l'AI Act non impone di nominare un "AI Officer", ma richiede provider e deployer di assicurare, per quanto possibile, un livello sufficiente di AI literacy del personale e delle persone che operano o utilizzano sistemi AI per loro conto. È quindi corretto evitare letture organizzative eccessivamente formalistiche: non è il titolo della funzione a contare, ma l'esistenza di responsabilità chiare, competenze adeguate, flussi decisionali documentati e controlli verificabili.

La conclusione operativa è che non basta un comitato AI di facciata. Serve una matrice RACI che attribuisca responsabilità a business owner, legal, compliance, DPO, CISO, risk management, procurement, internal audit e funzioni di controllo. Per le imprese vigilate, la collocazione naturale è dentro i framework già esistenti: comitati rischi, product governance, outsourcing committee, model risk committee, data governance forum, ICT risk governance.

Una buona policy AI per banche e assicurazioni dovrebbe contenere almeno quattro livelli.

Il primo è il livello di divieto: usi non ammessi, inclusi social scoring, manipolazione dannosa, sfruttamento di vulnerabilità, emotion recognition vietata nel workplace, biometric categorisation per inferire caratteristiche sensibili, scraping non mirato di immagini facciali e pratiche predatorie verso clienti vulnerabili.

Il secondo è il livello di approvazione rafforzata: casi d'uso in credito, pricing assicurativo, underwriting, HR, customer profiling, reclami, AML, fraud management, recupero crediti, consulenza automatizzata e sistemi agentici con capacità di azione.

Il terzo è il livello di controllo continuo: logging, monitoraggio performance, drift, bias testing, human oversight, incident escalation, revisione dei prompt e dei dataset, gestione versioni, audit trail.

Il quarto è il livello contrattuale: clausole vendor, diritti di audit, documentazione tecnica, change notification, cybersecurity, subfornitura, localizzazione e accesso ai dati, proprietà intellettuale, uso dei dati per training, responsabilità in caso di output errati o discriminatori.

La centralizzazione di alcune competenze presso l'AI Office non elimina la rilevanza delle autorità settoriali. Anzi, per le financial institutions l'accordo sul Digital Omnibus conferma la necessità di coordinare AI governance e vigilanza finanziaria, perché la supervisione AI non potrà essere letta in modo isolato rispetto a prudential supervision, conduct supervision, DORA, outsourcing e product governance.

7. Ciò che il rinvio non risolve: GPAI, LLM e procurement di soluzioni AI

Il Digital Omnibus rischia di essere letto dagli operatori come un rinvio generalizzato della compliance AI. Per le istituzioni finanziarie e assicurative questa lettura sarebbe fuorviante, soprattutto rispetto ai modelli general-purpose e alle soluzioni LLM già integrate nei processi aziendali. Il problema non è solo quando diventeranno pienamente applicabili gli obblighi high-risk, ma come l'intermediario governa oggi l'acquisto, l'integrazione e l'utilizzo di modelli forniti da terzi, spesso incorporati in servizi cloud, SaaS, piattaforme di customer management, strumenti antifrode, soluzioni di underwriting o sistemi di produttività aziendale.

vedi l'articolo online

Banche e assicurazioni stanno sperimentando modelli general-purpose per assistenza documentale, customer service, supporto alla compliance, analisi contrattuale, gestione sinistri, underwriting, formazione, codifica software, reportistica e knowledge management. L'AI Act distingue tra modelli GPAI, sistemi AI che li integrano e responsabilità degli attori lungo la value chain. Le linee guida e il Code of Practice evidenziano che i modelli GPAI hanno un ruolo particolare perché possono essere integrati in molti sistemi downstream e perché i provider devono fornire informazioni utili ai downstream provider e, su richiesta, all'AI Office.

Il Code of Practice sul capitolo Transparency è, per gli intermediari, una miniera di indicazioni da tradurre in procurement checklist. Prevede model documentation, informazioni per downstream provider e autorità, aggiornamento della documentazione, conservazione delle versioni precedenti e misure di qualità, sicurezza e integrità delle informazioni. Il capitolo Copyright, invece, richiama la necessità per i provider GPAI di predisporre una copyright policy, rispettare riserve di diritti nel text and data mining e rendere disponibili sintesi sui contenuti usati per il training.

Per una banca o una compagnia assicurativa, ciò significa che l'acquisto di un LLM non può essere gestito come una normale licenza SaaS. Le clausole dovrebbero coprire almeno: descrizione del modello e delle sue capacità; documentazione tecnica disponibile; data sources e policy sul training; uso dei dati del cliente per training o fine-tuning; misure contro hallucination e output dannosi; logging e explainability; incident notification; cybersecurity; audit; change management; garanzie IP; responsabilità su contenuti generati; localizzazione e trasferimenti dati; subprocessor; exit; continuità operativa; integrazione con DORA e outsourcing.

Il tema è ancora più rilevante per gli AI agents. Le FAQ della Commissione chiariscono che gli agenti AI non sono una categoria autonoma dell'AI Act, ma di regola possono essere sia sistemi AI sia includere un modello GPAI; la capacità di ricevere input, usare strumenti, eseguire azioni e interagire con l'ambiente può incidere sulla valutazione dei rischi, inclusi rischi sistemici e high-risk.

Operativamente, gli intermediari dovrebbero trattare ogni soluzione agentica come un processo delegato: definire quali azioni può compiere senza approvazione umana, quali richiedono four-eyes principle, quali sono vietate; limitare accesso a sistemi core; imporre sandboxing; mantenere audit trail; prevedere kill switch; monitorare prompt injection, data leakage e tool misuse; vietare decisioni automatiche con effetti giuridici o economici significativi sul cliente senza controllo umano effettivo.

In fase di procurement, la domanda non dovrebbe più essere soltanto "il fornitore è conforme all'AI Act?", ma: il fornitore è in grado di mettere l'intermediario nelle condizioni di dimostrare la propria compliance, ricostruire le decisioni, gestire incidenti, rispondere a clienti e autorità, e preservare segreti, dati personali e continuità operativa?

8. Dati, bias e GDPR: il Digital Omnibus non elimina il problema, lo rende più esplicito

Uno degli elementi più discussi del Digital Omnibus è l'apertura al trattamento di categorie particolari di dati personali per finalità di bias detection e correction, soggetta a garanzie. La Commissione presenta questa misura come funzionale a rendere più efficace la compliance AI, ma EDPB ed EDPS hanno raccomandato che l'utilizzo di tali dati resti fondato su un criterio di stretta necessità e non diventi un'autorizzazione generale al trattamento di dati sensibili.

Nel settore finanziario e assicurativo questo punto è particolarmente delicato. La correzione dei bias può richiedere di verificare effetti discriminatori su gruppi protetti, ma il trattamento di dati sensibili, proxy o informazioni inferite può a sua volta generare nuovi rischi. Il bilanciamento non può essere risolto con una clausola privacy standard.

Le istituzioni dovrebbero predisporre un "bias testing protocol" integrato con DPIA e, se applicabile, fundamental rights impact assessment. Il protocollo dovrebbe definire: quali rischi discriminatori sono ragionevolmente prevedibili; quali dati sono strettamente necessari per testarli; se esistono alternative meno intrusive; chi accede ai dati; per quanto tempo; con quali misure di segregazione; come si evita che il dato sensibile usato per testing rientri nel modello operativo; come vengono documentate decisioni e remediation.

Nel credito, esempi classici includono l'uso di postcode, professione, pattern di spesa, device data o canali di acquisizione come proxy di condizioni socio-economiche o appartenenze protette. Nell'assicurazione vita e salute, il rischio è ancora più evidente: dati sanitari, inferenze genetiche, acquisti farmaceutici, wearable data o informazioni comportamentali possono incidere su pricing, esclusioni o

vedi l'articolo online

condizioni contrattuali.

Il suggerimento operativo è non aspettare gli standard tecnici per predisporre una documentazione difendibile: per ogni modello rilevante dovrebbero esistere una data lineage, un registro delle variabili, una valutazione dei proxy, test di fairness, decisioni di esclusione o inclusione delle feature, controlli su drift e documentazione delle remediation. Questa documentazione dovrebbe essere pensata non solo per il regulator AI, ma anche per DPO, funzione compliance, internal audit, autorità di vigilanza finanziaria e gestione del contenzioso.

9. Incident reporting, DORA e AI: verso un playbook unico

Il Digital Omnibus si inserisce in un ecosistema regolamentare già molto denso. La BCE, nel proprio parere sul pacchetto, ha sostenuto l'obiettivo di semplificazione e competitività, ma ha anche richiamato l'esigenza di mantenere standard elevati e di gestire la complessità e le sovrapposizioni delle regole digitali UE. Il pacchetto tocca anche profili di coordinamento tra NIS2 e DORA, in particolare nella prospettiva di un possibile single-entry point per alcuni obblighi di reporting.

Le draft guidance sull'articolo 73 AI Act confermano il punto: il serious incident reporting per sistemi high-risk può sovrapporsi a DORA, GDPR, NIS2 e altri regimi. Per le financial entities soggette a DORA, se un sistema AI rientrante nei casi 5(b) o 5(c) dell'Allegato III è anche rilevante ai fini di incidenti ICT, potranno emergere obblighi paralleli o aggiuntivi, in particolare quando vi siano violazioni di diritti fondamentali.

Per le financial entities soggette a DORA, l'incidente AI sarà spesso anche un incidente ICT, un data breach, un problema di condotta o un evento rilevante per i diritti fondamentali. La compliance non dovrebbe quindi creare un reporting AI separato, ma un playbook integrato AI-DORA-GDPR-NIS2: classificazione dell'evento, conservazione dei log, blocco o rollback del modello, escalation a CISO, DPO, compliance e legal, valutazione dell'impatto sul cliente e coordinamento delle notifiche alle autorità.

In questa prospettiva, l'AI Act dovrebbe essere trattato come un'estensione del digital operational resilience framework, non come un allegato separato. Per un intermediario, il punto non è solo sapere quando notificare, ma essere in grado di ricostruire cosa è accaduto: quale versione del modello era in uso; quali dati erano stati utilizzati; quali soglie decisionali erano state impostate; quali controlli umani erano previsti; quali log sono disponibili; quali clienti sono stati impattati; quali misure correttive sono state adottate.

Questo approccio consente anche di evitare duplicazioni organizzative: l'AI incident management può essere integrato con crisis management, business continuity, ICT risk management, outsourcing governance e procedure di gestione reclami.

10. Una roadmap in dieci mosse per banche e assicurazioni

La semplificazione del Digital Omnibus dovrebbe essere tradotta in un piano operativo con scadenze interne, non solo regolamentari.

Primo: definire una AI risk appetite statement approvata a livello adeguato, chiarendo usi vietati, usi soggetti ad approvazione rafforzata e usi ordinari.

Secondo: completare un inventario AI enterprise-wide, includendo strumenti vendor, sistemi embedded, proof of concept, soluzioni di gruppo, strumenti HR e modelli GPAI.

Terzo: classificare i casi d'uso sulla base di "intended purpose", ruolo dell'ente, impatto sul cliente, dati utilizzati e dipendenza decisionale, documentando perché un sistema è high-risk, non high-risk o fuori perimetro.

Quarto: predisporre un assessment specifico per credito e assicurazione vita/salute, distinguendo scoring, creditworthiness, anti-frode, prudential models, product design, underwriting, pricing, claims e complaints.

Quinto: integrare AI governance con DORA e outsourcing, rivedendo contratti con fornitori ICT, cloud, SaaS, model providers e system integrator.

Sesto: introdurre controlli minimi per GPAI e agentic AI: data isolation, prompt governance, human approval, logging, output validation, IP safeguards, cyber controls e limiti funzionali.

Settimo: creare un protocollo dati e bias che coordini GDPR, AI Act, DPIA, FRIA, data minimisation e testing di non discriminazione.

Ottavo: aggiornare product governance e customer communication, soprattutto per prodotti creditizi, assicurativi, consulenza automatizzata, chatbot e reclami.

Nono: predisporre un incident playbook AI-DORA-GDPR, con scenari discriminazione, malfunzionamento, data breach, hallucination materiale, output ingannevole, decisione errata e reclamo massivo.

Decimo: formare il personale per ruolo. La formazione generica sull'AI non basta: servono percorsi differenziati per board, funzioni di controllo, procurement, sviluppatori, data scientist, business owner, relationship manager, underwriter, claims handler e customer care.

A queste dieci mosse occorre aggiungere una cautela di calendario: le scadenze esterne non dovrebbero coincidere con le scadenze interne. Se l'obiettivo è essere pronti al 2 dicembre 2027 per molti sistemi Annex III, le decisioni su inventario, classificazione, procurement, data governance e incident management devono essere prese ben prima. La compliance AI non si costruisce alla vigilia dell'entrata in applicazione: richiede cicli di remediation contrattuale, tecnica e organizzativa.

11. Conclusioni: il vantaggio competitivo sarà nella compliance industrializzata

Il Digital Omnibus è stato presentato come semplificazione, ma per banche e assicurazioni la vera semplificazione non arriverà solo dal legislatore. Arriverà dalla capacità di trasformare l'AI compliance in un framework industrializzato, integrato con controlli già esistenti e proporzionato ai rischi reali.

Gli operatori che useranno il rinvio per attendere rischiano di trovarsi, alla nuova scadenza, con lo stesso problema di oggi: sistemi non inventariati, contratti non adeguati, ruoli non chiari, dati non tracciati, bias non testati, incidenti non classificabili e controlli umani solo nominali.

Gli operatori che useranno il tempo per costruire un AI control framework potranno invece ottenere un duplice risultato: ridurre il rischio regolamentare e accelerare l'adozione sicura dell'AI. Per istituzioni finanziarie e assicurative, questo è il punto centrale: l'AI Act non è solo una norma di compliance, ma un test di maturità della governance digitale.

La semplificazione, in definitiva, non riduce l'importanza della compliance: la sposta dal piano dell'urgenza formale al piano della capacità organizzativa. Per banche, intermediari e assicurazioni, il Digital Omnibus è quindi un'occasione da non sprecare: usare il tempo aggiuntivo non per rinviare, ma per rendere l'AI governabile, auditabile, contrattualmente presidiata e coerente con il più ampio sistema europeo di resilienza digitale, tutela dei dati, condotta di mercato e protezione dei diritti fondamentali.

vedi l'articolo online

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it