Digital Omnibus (COM(2025) 837) , proposta della Commissione del 19.11.2025

A cura di Stefano Gorla e Valeria Lazzaroli

ENTE NAZIONALE PER L'INTELLIGENZA ARTIFICIALE
ENIA

Digital Omnibus (COM(2025) 837) – proposta della Commissione – 19 novembre 2025

La proposta di Regolamento "Digital Omnibus" presentata dalla Commissione europea introduce un intervento strutturale sull'intero quadro normativo digitale dell'Unione. L'obiettivo dichiarato è duplice: garantire coerenza sistemica e ridurre gli oneri amministrativi, preservando al contempo il livello di tutela che negli ultimi anni ha definito lo standard europeo in materia di dati, privacy e sicurezza informatica.

L'operazione mira a riunificare in un unico corpus norme oggi disperse in atti distinti. Le disposizioni su open data, governance dei dati e libera circolazione dei dati non personali confluiscono così nel Data Act, che diviene il fulcro del nuovo *acquis* digitale. Contestualmente, il perimetro relativo all'accesso pubblico ai dati detenuti da soggetti privati viene ridefinito con precisione, limitando gli obblighi di condivisione alle sole situazioni che configurano una vera emergenza pubblica. Le tutele dei segreti commerciali vengono rafforzate, con un'attenzione specifica ai rischi connessi a giurisdizioni extra-UE caratterizzate da sistemi di protezione insufficienti.

Il capitolo dedicato ai servizi cloud viene ricalibrato per tenere conto delle esigenze dei servizi altamente personalizzati e dei fornitori di dimensioni ridotte o medie, riconoscendo la necessità di un percorso di transizione graduale verso il pieno superamento dei vincoli allo switching. Sul fronte della protezione dei dati personali, il testo interviene su alcuni nodi interpretativi emersi nell'applicazione del GDPR: chiarimenti sulla nozione di dato personale, semplificazione delle informative in scenari a basso rischio, revisione dei criteri di notifica dei data breach, definizione di template comuni per le DPIA e chiarimenti sull'uso di processi decisionali automatizzati. La disciplina relativa ai cookie viene trasposta all'interno del GDPR, con l'introduzione di segnali di scelta *machine-readable* destinati a diventare lo standard europeo.

Un capitolo autonomo è dedicato alla gestione delle notifiche di incidenti in materia di cybersicurezza, con l'istituzione di un canale unico europeo affidato a ENISA, che consente un'unica trasmissione valida per più regimi normativi. Si chiude infine la stagione del Regolamento P2B, ormai superato dal nuovo quadro delineato da DSA e DMA.

L'impatto complessivo dell'intervento è stimato in un risparmio di almeno un miliardo di euro all'anno, cui si aggiunge un beneficio una tantum di pari entità, con un effetto cumulato di circa cinque miliardi entro il 2029. In prospettiva, il Digital Omnibus consolida il modello europeo e rafforza la competitività del mercato unico, evitando sovrapposizioni normative e promuovendo un approccio più lineare, leggibile e funzionale alla transizione digitale.

Novità principali

Riunificazione della normativa sui dati nel Data Act	La proposta concentra in un unico corpo normativo il Data Governance Act, la Open Data Directive e il regolamento sulla libera circolazione dei dati non personali. Il divieto di localizzazione dei dati viene confermato e inserito stabilmente nel Data Act, superando l'attuale frammentazione e garantendo maggiore coerenza applicativa.
Ridefinizione del perimetro di accesso pubblico ai dati privati (B2G)	Gli obblighi di condivisione sono limitati alle sole situazioni qualificabili come "emergenze pubbliche". Sono chiariti i criteri per la determinazione dei compensi dovuti ai detentori dei dati e viene rivisto il regime per l'utilizzo statistico da parte delle autorità pubbliche.
Rafforzamento delle garanzie sui segreti commerciali	Il detentore dei dati può rifiutare la condivisione quando sussista un rischio elevato di acquisizione o divulgazione verso Paesi terzi che non assicurano un livello adeguato di protezione. Il rifiuto deve essere motivato e comunicato all'autorità competente.
Revisione del quadro dedicato agli smart contracts	Vengono eliminati i requisiti essenziali previsti dall'articolo 36 del Data Act e la relativa procedura di valutazione ex ante. La Commissione conserva la possibilità di definire standard armonizzati in una fase successiva, alla luce dell'evoluzione tecnologica.
Semplificazione del regime sul cloud switching	Per i servizi fortemente personalizzati e per i fornitori di piccole e medie dimensioni — inclusi gli small mid-cap — operanti su contratti stipulati prima del 12 settembre 2025, è previsto un regime meno oneroso. Resta fermo l'obiettivo europeo di eliminare progressivamente costi e barriere allo switching, incluse le egress charges.
Unificazione delle regole sul riutilizzo dei dati della PA	Open data e dati protetti confluiscono in un unico quadro operativo. Le pubbliche amministrazioni possono applicare condizioni economiche più elevate nei confronti delle very large enterprises, come i gatekeeper, purché fondate su criteri oggettivi e trasparenti. Sono inoltre rafforzati i punti informativi unici.
Interventi mirati sul GDPR	La definizione di dato personale viene chiarita con riferimento ai mezzi ragionevolmente disponibili per identificare una persona. Sono introdotte deroghe calibrate per attività di ricerca, sviluppo di sistemi di intelligenza artificiale e verifiche biometriche in modalità "uno-a-uno". Le informative possono essere semplificate in scenari a basso rischio. La notifica dei data breach è richiesta solo in caso di rischio elevato, con un termine di 96 ore e con l'utilizzo del single-entry point europeo. Le DPIA saranno supportate da liste e template armonizzati a livello UE. Sono inoltre precisate le condizioni per l'uso di processi decisionali automatizzati.
Migrazione della disciplina sui cookie nel GDPR	La regolamentazione sull'accesso e sulla memorizzazione di informazioni nei terminali degli utenti è trasferita nei nuovi articoli 88a e 88b del GDPR. I sistemi dovranno accettare segnali standardizzati di consenso o diniego, una volta definiti. È previsto un regime speciale per i media service providers.

Istituzione del Single Entry Point europeo per le notifiche di incidenti	ENISA diventa il punto di ingresso unico per le notifiche previste da NIS2, GDPR, DORA, eIDAS e CER. Il principio operativo è "report once, share many", con riutilizzo dei template già adottati in ambito DORA per garantire uniformità e ridurre gli oneri per gli operatori.
Superamento del Regolamento P2B	Il regolamento (UE) 2019/1150 viene abrogato, poiché le materie da esso disciplinate sono ora coperte dal nuovo assetto definito dal Digital Services Act e dal Digital Markets Act. Alcune disposizioni continuano a produrre effetti transitori fino al 31 dicembre 2032, per garantire coerenza con rinvii presenti in altri atti.

Consolidamento e calibrazione del "data acquis" (Data Act)

La proposta di Regolamento interviene in modo organico sulla disciplina europea dei dati, superando la frammentazione che negli ultimi anni ha reso complesso il quadro applicativo. Il Data Act diventa l'asse portante dell'intero sistema, assumendo al proprio interno contenuti che, fino ad oggi, trovavano sede in atti distinti.

Confluenza normativa

Il Data Governance Act (Reg. UE 2022/868), il regolamento sul libero flusso dei dati non personali (Reg. UE 2018/1807) e la Open Data Directive (Dir. 2019/1024) vengono formalmente abrogati, con integrale trasposizione dei relativi contenuti nel Data Act. Il divieto di localizzazione dei dati non personali è confermato e ricollocato in un quadro più ampio e coerente, finalizzato a garantire continuità operativa nel mercato unico e certezza applicativa per operatori pubblici e privati.

Nuovi capitoli incorporati nel Data Act

– *Capitolo VIIa.* Le attività di intermediazione dei dati e le iniziative di data altruism assumono carattere volontario. Gli obblighi previsti dal precedente regime vengono significativamente ridotti: la separazione richiesta non è più di natura giuridica, ma funzionale, con un alleggerimento sostanziale per le organizzazioni interessate.
– *Capitolo VIIb.* Il divieto di data localisation, già contenuto nel FFDR, è integrato direttamente nel Data Act. Contestualmente, vengono semplificati gli adempimenti previsti a livello nazionale, così da evitare sovrapposizioni e interpretazioni divergenti.
– *Capitolo VIIc.* Si introduce un quadro unico per il riutilizzo dei dati detenuti dalle pubbliche amministrazioni. I principi di non discriminazione, assenza di esclusività e disponibilità in formato *machine readable* degli high value datasets diventano uniformi a livello europeo. È inoltre previsto un punto informativo unico, destinato a facilitare l'accesso e la trasparenza.

Tarature e adeguamenti mirati

Il nuovo testo rafforza le tutele relative ai segreti commerciali nell'ambito della condivisione dei dati generati da dispositivi IoT, prevedendo misure più rigorose a protezione degli interessi industriali. Il perimetro delle richieste B2G viene precisato per evitare utilizzi impropri dello strumento. Sono soppressi gli "essential requirements" precedentemente previsti per gli smart contracts, sostituiti da una competenza regolatoria affidata alla Commissione, che potrà intervenire con standard armonizzati qualora necessario.
In materia di servizi cloud, il regime di switching è alleggerito per i servizi con elevata personalizzazione e per i fornitori di piccole e medie dimensioni, inclusi gli small mid-cap, ai quali viene riconosciuta una transizione più equilibrata verso il nuovo modello competitivo europeo.

Privacy e protezione dati (GDPR & ePrivacy)

La proposta interviene su un insieme di nodi interpretativi e operativi che, negli anni, hanno reso l'applicazione del GDPR disomogenea nel territorio dell'Unione. Le modifiche non alterano i principi fondanti del regolamento, ma ne precisano l'ambito applicativo, introducendo strumenti di semplificazione destinati a garantire maggiore certezza giuridica per titolari e responsabili del trattamento.

Chiarimenti definitori

Sono precisati i criteri che consentono di stabilire quando un dato pseudonimizzato possa essere considerato, nei fatti, non personale. L'elemento determinante diventa la disponibilità di mezzi ragionevoli per procedere all'identificazione. Questo orientamento uniforma la pratica amministrativa e riduce il rischio di eccesso di cautela da parte degli operatori.

Disciplina degli incidenti di sicurezza

L'obbligo di notifica alle autorità di controllo è circoscritto ai casi in cui l'incidente sia suscettibile di generare un rischio elevato per i diritti e le libertà delle persone interessate. Il termine per effettuare la notifica viene portato a 96 ore. La comunicazione dovrà transitare attraverso il *single entry point* europeo, utilizzando i template armonizzati predisposti dall'EDPB e adottati dalla Commissione tramite atti esecutivi. L'impianto mira a ridurre la duplicazione di comunicazioni e a migliorare la qualità informativa delle segnalazioni.

Valutazioni d'impatto (DPIA)

Sono introdotte liste armonizzate di trattamenti che richiedono, o non richiedono, la valutazione d'impatto ai sensi dell'articolo 35 del GDPR. Tali liste, unitamente ai modelli

e alle metodologie comuni proposti dall'EDPB, consentiranno alle organizzazioni di uniformare i processi interni e ridurre gli scostamenti interpretativi tra Stati membri.

Processi decisionali automatizzati (articolo 22)

Viene chiarito il significato del requisito di "necessità" quando una decisione automatizzata è adottata nell'ambito dell'esecuzione di un contratto. La necessità può essere riconosciuta anche quando la medesima decisione potrebbe essere assunta da un operatore umano, purché l'automazione rappresenti la soluzione più proporzionata e meno invasiva, a parità di risultati.

Cookie e altri strumenti analoghi

La disciplina oggi contenuta nella normativa ePrivacy viene trasferita nel GDPR, attraverso l'introduzione del nuovo articolo 88a. È inoltre previsto il nuovo articolo 88b, che introduce segnali di consenso e opposizione *machine readable*, destinati a essere integrati nativamente in browser e dispositivi. Si tratta di una misura strutturale volta a superare la frammentazione attuale e ridurre la cosiddetta *cookie fatigue*, favorendo scelte più chiare, trasparenti e standardizzate.

Cybersecurity e incident reporting (NIS2, DORA, CER, eIDAS)

Il capitolo dedicato alla cybersicurezza affronta uno dei temi più complessi dell'attuale quadro regolatorio europeo: la molteplicità di obblighi di notifica che ricadono su imprese e pubbliche amministrazioni, spesso in modo sovrapposto. La proposta interviene in modo strutturale, introducendo un punto unico di ingresso che unifica procedure, modelli e responsabilità, con l'obiettivo di migliorare il coordinamento e ridurre gli oneri amministrativi.

Single Entry Point europeo

La direttiva NIS2 viene integrata mediante l'introduzione del nuovo articolo 23a, che attribuisce a ENISA la responsabilità di progettare, gestire e mantenere un portale digitale unico per la trasmissione delle notifiche di incidente. Una comunicazione inviata attraverso tale canale diviene valida simultaneamente per i regimi previsti da NIS2, GDPR (per i data breach), DORA, CER ed eIDAS, incluse le attività relative ai trust services. L'infrastruttura sarà interoperabile con le European Business Wallets, garantendo un flusso dati standardizzato e verificabile.

Obbligatorietà dell'uso del canale unico

La disciplina NIS2 viene modificata per rendere obbligatorio, per gli operatori che subiscono incidenti significativi, l'utilizzo del single entry point. Il principio del "once only", già recepito nel Cyber Resilience Act, viene così applicato anche al sistema delle notifiche di sicurezza. Il portale accoglierà inoltre segnalazioni volontarie, utili per

stimolare la cooperazione informativa tra operatori e autorità competenti. Le modifiche puntuali al testo NIS2 sono illustrate nel documento alle pagine 90–91 della proposta.

Coordinamento con DORA

Il regime DORA, che disciplina gli incidenti ICT nel settore finanziario, è integrato all'interno di questa architettura comune. Gli incidenti maggiori di cui all'articolo 19 e le segnalazioni volontarie relative a minacce informatiche transiteranno anch'essi attraverso il single entry point. I modelli informativi utilizzati negli altri regimi (NIS2, CER, GDPR) saranno allineati a quelli già introdotti da DORA, assicurando uniformità metodologica e riducendo gli sforzi di adattamento per gli operatori.

Attivazione della piattaforma

ENISA è tenuta a completare lo sviluppo del portale entro diciotto mesi dall'entrata in vigore del Digital Omnibus. L'utilizzo effettivo diventerà obbligatorio solo dopo la pubblicazione in Gazzetta Ufficiale dell'avviso della Commissione che ne attesti la piena operatività. Tale meccanismo garantisce una transizione ordinata e consente agli operatori di predisporre in tempo utile le integrazioni tecniche necessarie.

AI Act

Il Digital Omnibus interviene sull'AI Act con un atto separato di modifica, concepito non per riscrivere l'impianto della disciplina, ma per renderne più gestibile l'attuazione in una fase in cui il tessuto produttivo europeo deve ancora assestarsi rispetto agli obblighi introdotti dal Regolamento (UE) 2024/1689. L'azione si sviluppa su due assi principali: semplificazione dell'implementazione tecnica e amministrativa, in particolare per PMI e *small mid-caps*, e chiarificazione del rapporto tra AI Act e GDPR nella fase di addestramento e sviluppo dei sistemi.

Misure di facilitazione per l'attuazione dell'AI Act

La proposta Omnibus è accompagnata da un regolamento di modifica dell'AI Act che introduce un insieme di aggiustamenti mirati, con tre obiettivi operativi:

Dare priorità agli standard e alle linee guida essenziali	La Commissione, attraverso l'AI Office e gli organismi europei di normazione, viene chiamata a definire una sequenza chiara di standard armonizzati e linee guida prioritarie. In particolare, sono messi in cima all'agenda:

	○ gli standard relativi ai sistemi di AI ad alto rischio, con riguardo ai requisiti di gestione del rischio, qualità dei dati, documentazione tecnica e tracciabilità; ○ gli standard per i sistemi di AI general purpose, inclusi gli obblighi di *content labelling* e watermarking già previsti dall'AI Act, che necessitano di specifiche tecniche condivise per essere applicati in modo uniforme; ○ le linee guida interpretative sulle responsabilità lungo la catena del valore (fornitori di modelli di base, integratori, deployer), per ridurre il rischio di scarico improprio degli oneri regolatori su un unico anello della filiera.
Scaglionare gli obblighi temporali e alleggerire la prima fase applicativa	Per i fornitori di sistemi di AI ad alto rischio, in particolare in ambiti sensibili (occupazione, credito, sanità, esami, biometria, law enforcement), sono previsti margini temporali aggiuntivi per l'adeguamento agli obblighi più complessi, nel solco delle ipotesi di rinvio dell'entrata in piena applicazione fino al 2027 per alcune categorie di requisiti. In parallelo, è rafforzato il ruolo dell'AI Office come punto di coordinamento centrale per: ○ elaborare *guidance* comuni; ○ promuovere schemi di documentazione standard; ○ favorire convergenza tra autorità nazionali competenti, riducendo interpretazioni divergenti che aggraverebbero l'onere per le imprese transfrontaliere.
Riduzione dei carichi amministrativi superflui	Le modifiche puntano a distinguere con maggiore nettezza tra obblighi sostanziali (sicurezza, robustezza, mitigazione dei rischi per i diritti fondamentali) e adempimenti puramente formali. Dove possibile, la documentazione richiesta viene resa più modulare e proporzionata al tipo di sistema, con l'obiettivo di consentire l'uso di *template* comuni invece di dossier costruiti ogni volta da zero.

Regime alleggerito per PMI e *small mid-caps*

Accanto al regime agevolato già previsto dall'AI Act per micro e piccole imprese, l'Omnibus introduce ulteriori misure specifiche per le *small mid-caps*, riconoscendo che una parte rilevante dell'innovazione europea in ambito AI è concentrata in realtà che, pur non essendo micro, non dispongono delle risorse organizzative delle grandi imprese.

In questo quadro, sono previste tre direttrici:

Proporzionalità rafforzata nella conformità	Per PMI e *small mid-caps*: o le procedure di valutazione di conformità possono avvalersi in misura maggiore di schemi semplificati, linee guida e modelli predisposti a livello UE; o la frequenza e la granularità di alcuni obblighi di reporting e aggiornamento della documentazione sono tarate in ragione del rischio effettivo del sistema e dell'impatto sul mercato, evitando duplicazioni rispetto ad altri regimi (ad esempio in ambito DORA o NIS2, quando applicabili).
Ricorso sistematico alla standardizzazione	Lo strumento degli standard armonizzati è esplicitamente indicato come via preferenziale per consentire alle imprese di dimostrare la conformità "per relationem", riducendo il contenzioso interpretativo. Per le *small mid-caps*, ciò significa poter impostare processi interni una volta sola, costruendoli sui riferimenti tecnici comuni, invece di dover ricostruire autonomamente il senso di ogni obbligo.
Supporto operativo e coordinamento con sandbox e misure di sostegno	Le modifiche richiamano espressamente: o la necessità di coordinare l'attuazione dell'AI Act con i programmi di *AI sandbox* e con gli strumenti di sostegno all'innovazione previsti a livello unionale e nazionale; o il ruolo delle autorità competenti nel fornire chiarimenti preventivi (ad esempio, tramite Q&A pubbliche, modelli di registri, esempi di DPIA coerenti con gli obblighi dell'AI Act), così da evitare che l'incertezza normativa diventi essa stessa un fattore di rischio per le imprese di media dimensione.

Interplay con il GDPR: liceità dei trattamenti per addestramento e sviluppo AI

Uno degli aspetti più delicati dell'Omnibus riguarda il rapporto tra AI Act e GDPR nei trattamenti di dati personali destinati all'addestramento, validazione e aggiornamento dei sistemi di intelligenza artificiale.

Chiarimento delle basi giuridiche per l'addestramento AI	Il testo mira a specificare in quali condizioni il legittimo interesse del titolare possa costituire base giuridica per l'uso di dati personali a fini di addestramento dei modelli, anche in assenza di consenso individuale, purché: o siano adottate misure robuste di minimizzazione e pseudonimizzazione; o sia condotta una valutazione d'impatto (DPIA) quando il rischio complessivo lo richiede; o siano previste modalità effettive di esercizio dei diritti, inclusa la possibilità di opposizione nei casi previsti dal GDPR. In questo modo si cerca di evitare che ogni uso di dati per scopi di training richieda necessariamente il consenso esplicito, mantenendo però un presidio sostanziale sui diritti degli interessati.
Coerenza nella gestione delle categorie particolari di dati	In linea con gli aggiustamenti proposti sul GDPR, il trattamento di categorie particolari di dati (salute, opinioni politiche, convinzioni religiose, ecc.) nei dataset AI viene ammesso solo in forma residuale e con cautele elevate, ad esempio: o obbligo di rimozione ove ragionevolmente possibile; o ricorso a tecniche di protezione avanzate (pseudonimizzazione forte, privacy differenziale, segregazione dei dataset); limitazione stretta degli accessi e dei riusi rispetto alla finalità originaria.
Allineamento tra obblighi AI Act e documentazione privacy	Gli obblighi documentali dell'AI Act (registri di sistema, descrizione delle pipeline di dati, misure di governance) e quelli del GDPR (registri dei trattamenti, DPIA, informative) vengono esplicitamente coordinati. L'obiettivo è consentire, in prospettiva, che:

	○ una singola DPIA, costruita secondo i *template* europei, possa coprire sia i profili di rischio AI Act sia quelli di protezione dati; ○ i registri dei trattamenti evidenzino con maggiore chiarezza quali componenti di un sistema rientrano nell'ambito di applicazione dell'AI Act e quali rimangono sotto il solo perimetro GDPR. Il capitolo AI Act del Digital Omnibus non modifica la logica di fondo del regolamento sull'intelligenza artificiale, ma introduce strumenti di "messa a terra" normativa che mirano a rendere praticabile l'adempimento, soprattutto per gli operatori di dimensioni medio-piccole, e a sciogliere i nodi più sensibili nell'intersezione tra sviluppo di sistemi AI e disciplina europea della protezione dei dati.

La proposta interviene su tre piani:

Misure ulteriori e coordinamento con altri strumenti dell'ecosistema digitale europeo

Il Digital Omnibus prevede anche interventi mirati su atti normativi che, per ragioni di evoluzione tecnologica e convergenza regolatoria, risultano ormai superati o necessitano di adeguamenti funzionali all'architettura complessiva introdotta dalla proposta.

Abrogazione del Regolamento P2B (Reg. UE 2019/1150)

Il regolamento sulle relazioni tra piattaforme online e utenti commerciali (P2B), entrato in vigore nel 2020 per rafforzare la trasparenza e l'equità dei servizi digitali intermediati, viene formalmente abrogato. La scelta della Commissione è motivata dal fatto che il P2B è stato, di fatto, superato dalla combinazione tra il Digital Services Act (DSA) e il Digital Markets Act (DMA). Le due normative, già pienamente applicabili, affrontano con maggiore ampiezza e profondità le dinamiche di trasparenza, responsabilità e riequilibrio del potere contrattuale nei rapporti tra piattaforme e operatori economici. Esse coprono:

- obblighi di disclosure e auditing per servizi di intermediazione online di dimensioni significative;
- misure di prevenzione e contrasto alle pratiche distorsive dei gatekeeper;
- limiti all'autopreferenziazione e alla discriminazione nell'accesso ai mercati digitali;
- obblighi specifici di interoperabilità e di portabilità dei dati.

Coerentemente, il P2B non è più necessario come atto autonomo. Alcune sue disposizioni rimangono tuttavia operative fino al 31 dicembre 2032, nella sola misura in cui

costituiscono riferimenti incrociati in atti europei che non sono ancora stati modificati. Tali residui normativi sono destinati a scomparire progressivamente attraverso l'aggiornamento sistematico dell'acquis.

Integrazione con le European Business Wallets

La proposta valorizza il ruolo delle *European Business Wallets* (EBW), l'infrastruttura europea di identità e attestazioni digitali per imprese e operatori economici. Queste wallet, previste nell'ambito del nuovo quadro eIDAS, sono destinate a diventare uno strumento comune di autenticazione e identificazione nei rapporti con la pubblica amministrazione e tra operatori transfrontalieri. Nell'ambito del Digital Omnibus, le EBW assumono un ruolo specifico nel funzionamento del **single entry point** per la notifica degli incidenti di cybersicurezza e dei data breach. L'interoperabilità tra SEP ed EBW consente:

- **identificazione univoca e verificabile** del soggetto notificante, con riduzione del rischio di errori o di informazioni incomplete;
- **automatizzazione di parti del processo** di segnalazione, grazie alla possibilità di precompilare informazioni tramite attestazioni digitali già presenti nella wallet;
- **allineamento con gli standard di sicurezza europei**, evitando soluzioni tecniche eterogenee nei diversi Stati membri;
- **integrazione futura con altri servizi digitali**, inclusi gli adempimenti previsti dal Data Act per i riutilizzatori di dati pubblici e i soggetti coinvolti in processi di interoperabilità avanzata.

Questo collegamento strutturale permette di consolidare l'approccio europeo basato sul principio "*secure-by-design*" e di creare un ecosistema amministrativo in cui notifiche, autenticazione e tracciabilità seguano un percorso uniforme, verificabile e coerente.

Tabella di confronto – Regime attuale / Novità introdotte dal Digital Omnibus / Soggetti interessati / Impatto atteso

Data Act – Integrazione DGA / ODD / FFDR

Regime attuale:
Il quadro europeo dei dati risulta distribuito in tre atti distinti: il Data Governance Act, la Open Data Directive e il regolamento sul libero flusso dei dati non personali. Tale

frammentazione crea sovrapposizioni, obblighi duplicati e margini interpretativi incoerenti.

Cosa cambia:
Le tre normative vengono abrogate e trasfuse nel Data Act, che incorpora disposizioni su intermediazione dati, data altruism (con regime volontario e separazione funzionale), divieto di localizzazione e riuso dei dati pubblici, includendo high-value datasets e un sistema informativo unico.

Chi è interessato:
Pubbliche amministrazioni, intermediari, organismi di altruismo dei dati, imprese che riutilizzano dataset pubblici.

Impatto atteso:
Riduzione delle ridondanze normative, semplificazione degli adempimenti e maggiore uniformità delle definizioni operative.

Accesso pubblico ai dati privati (B2G) – Emergenze pubbliche

Regime attuale:
Il Data Act prevede un ampio concetto di "eccezionale necessità", che può generare richieste invasive e non sempre proporzionate.

Cosa cambia:
Il nuovo articolo 15a limita le richieste pubbliche ai casi qualificabili come vere emergenze pubbliche. È introdotta una disciplina più chiara su compensi e modalità d'uso dei dati personali, che devono essere pseudonimizzati quando possibile.

Chi è interessato:
Pubbliche amministrazioni, detentori di dati industriali e IoT.

Impatto atteso:
Riduzione degli oneri ingiustificati e certezza giuridica nella valutazione delle richieste B2G.

Segreti commerciali e Paesi terzi

Regime attuale:
Il rifiuto di condividere dati è ammesso solo se la divulgazione può causare un grave danno economico.

Cosa cambia:
La facoltà di rifiuto si estende ai casi in cui esista un rischio elevato di fuga, utilizzo

improprio o divulgazione verso giurisdizioni prive di tutele adeguate. Necessarie motivazione scritta e notifica all'autorità.

Chi è interessato:
Manifattura, produttori di dispositivi connessi, fornitori di servizi basati sui dati.

Impatto atteso:
Maggiore protezione degli asset industriali e dei vantaggi competitivi.

Smart Contracts nel Data Act

Regime attuale:
L'articolo 36 prevede requisiti essenziali e possibili valutazioni ex ante.

Cosa cambia:
L'articolo è abrogato. Eventuali requisiti tecnici saranno definiti tramite standard armonizzati della Commissione.

Chi è interessato:
Fornitori di soluzioni basate su registri distribuiti e applicazioni contrattuali automatizzate.

Impatto atteso:
Maggiore flessibilità tecnologica e riduzione delle incertezze.

Cloud Switching ed Egress Charges

Regime attuale:
Obblighi ampi di switching e progressiva eliminazione delle egress charges.

Cosa cambia:
Regime più leggero per servizi fortemente personalizzati e per PMI/SMC con contratti stipulati prima del 12 settembre 2025. Le penali di recesso anticipate sono ammesse se proporzionate. L'obiettivo di eliminare le egress resta invariato.

Chi è interessato:
Provider cloud, imprese clienti e pubbliche amministrazioni.

Impatto atteso:
Maggiore sostenibilità contrattuale per i provider, tutela avanzata nella portabilità per gli utenti.

Riuso dei dati della PA – Open & Protected Data

Regime attuale:
Coesistenza di ODD per gli open data e DGA per i dati protetti, con doppio binario operativo.

Cosa cambia:
La Sezione VIIc del Data Act unifica regole, principi e condizioni. Le PA possono applicare fee più elevate ai gatekeeper, sulla base di criteri oggettivi e documentabili.

Chi è interessato:
Pubbliche amministrazioni, riutilizzatori, grandi piattaforme, PMI e SMC.

Impatto atteso:
Accesso più trasparente e competitivo ai dati della PA.

Libera circolazione dei dati non personali

Regime attuale:
Il FFDR introduce il divieto di data localisation e un single information point nazionale.

Cosa cambia:
Il divieto viene trasferito nel Data Act; gli Stati membri non devono più gestire il punto informativo nazionale, riducendo la frammentazione burocratica.

Chi è interessato:
Fornitori e utenti di servizi basati sui dati.

Impatto atteso:
Maggiore armonizzazione procedurale.

Intermediazione e Altruismo dei dati

Regime attuale:
Regime obbligatorio di notifica e rulebook in via di sviluppo.

Cosa cambia:
Il riconoscimento diventa volontario, con registri europei e separazione funzionale. Eliminato il rulebook.

Chi è interessato:
Piattaforme di condivisione e organizzazioni non profit.

Impatto atteso:
Mercato più flessibile e meno oneroso.

GDPR – Definizione di dato personale

Regime attuale:
Interpretazioni divergenti su pseudonimizzazione e identificabilità.

Cosa cambia:
La nozione viene chiarita: un dato è personale solo se l'entità dispone di mezzi ragionevoli per identificare la persona. Indicazioni tecniche saranno definite a livello UE/EDPB.

Chi è interessato:
Titolari del trattamento, DPO, fornitori tecnologici.

Impatto atteso:
Riduzione delle letture iper-restrittive e maggiore certezza giuridica.

GDPR – Informative, accesso e data breach

Regime attuale:
Obblighi ampi, rischio di abusi del diritto di accesso e obbligo di notifica dei breach entro 72 ore.

Cosa cambia:
Informative semplificate in contesti a basso rischio; definizione degli abusi del diritto di accesso; notifica breach solo in caso di rischio elevato, entro 96 ore, tramite single entry point; DPIA su liste UE e template comuni.

Chi è interessato:
Tutti i titolari e i responsabili GDPR.

Impatto atteso:
Procedure più proporzionate e armonizzate.

Decisioni automatizzate (art. 22 GDPR)

Regime attuale:
Interpretazioni restrittive sulla "necessità" contrattuale.

Cosa cambia:
La necessità può sussistere anche se l'attività è astrattamente svolgibile da un umano, purché la soluzione automatizzata sia la meno intrusiva.

Chi è interessato:
Operatori che utilizzano sistemi di scoring o automazione decisionale.

Impatto atteso:
Migliore equilibrio tra innovazione e tutela.

AI e categorie particolari di dati

Regime attuale:
Incertezza sul ruolo dei dati sensibili residui nei dataset di addestramento.

Cosa cambia:
Deroga residuale con cautele elevate: rimozione ove possibile, protezione avanzata, valutazioni specifiche. Ammesso il legittimo interesse in condizioni rigorose.

Chi è interessato:
Fornitori di modelli, sviluppatori, deployer.

Impatto atteso:
Chiarezza operativa senza riduzione delle tutele.

Biometria – Verifica uno-a-uno

Regime attuale:
Quadro restrittivo sull'uso dei dati biometrici.

Cosa cambia:
Consentita la verifica uno-a-uno quando sotto esclusivo controllo dell'interessato (ad es. chiavi biometriche locali).

Chi è interessato:
Settori finanziario, telecomunicazioni, servizi digitali.

Impatto atteso:
Aumento dell'usabilità con rischio controllato.

Cookie e segnali dei browser (artt. 88a-88b GDPR)

Regime attuale:
Regole ePrivacy con banner eterogenei.

Cosa cambia:
La disciplina viene integrata nel GDPR, con segnali di consenso standardizzati. I media service provider sono esclusi dall'obbligo di rispettarli.

Chi è interessato:
Editori, ad-tech, sviluppatori di app.

Impatto atteso:
Standardizzazione europea e riduzione della *cookie fatigue*.

Single Entry Point per incidenti

Regime attuale:
Notifiche multiple e canali differenziati per NIS2, GDPR, DORA, CER, eIDAS.

Cosa cambia:
ENISA gestisce un unico portale europeo. Modelli mutuati da DORA. Attivazione prevista entro 18 mesi, prorogabile a 24.

Chi è interessato:
Operatori essenziali, settore finanziario, trust services, PA, imprese soggette a GDPR.

Impatto atteso:
Riduzione drastica degli oneri e migliore coordinamento istituzionale.

Regolamento P2B (2019/1150)

Regime attuale:
Disciplina autonoma delle relazioni piattaforma-business.

Cosa cambia:
Abrogazione. Rimangono solo rinvii transitori fino al 2032. Materia integralmente coperta da DSA e DMA.

Chi è interessato:
Marketplace, motori di ricerca, merchant online.

Impatto atteso:
Eliminazione delle sovrapposizioni normative.

Impatto economico complessivo

Regime attuale:
Oneri elevati dovuti a sovrapposizioni e frammentazione.

Cosa cambia:
Risparmi stimati superiori a 1 miliardo di euro l'anno, oltre a un beneficio una tantum di pari entità. Effetti cumulati attorno ai 5 miliardi entro il 2029.

Chi è interessato:
Imprese, PA, cittadini.

Impatto atteso:
Maggiore efficienza, competitività e slancio all'innovazione.

Prossime azioni consigliate (operatività)

Il Digital Omnibus richiede a imprese e amministrazioni un percorso di adattamento che non si esaurisce in un semplice aggiornamento documentale ma implica una ricognizione ampia delle relazioni contrattuali, dei processi IT e delle politiche interne di governance dei dati. Diventa quindi centrale avviare una mappatura accurata degli impatti, iniziando dai contratti che regolano servizi cloud, clausole sulle egress charges, condizioni di switching e protezione dei segreti commerciali, soprattutto quando coinvolgono trasferimenti verso Paesi terzi. Questo primo passaggio consente di comprendere dove intervenire e quali elementi necessitano di revisione.

Parallelamente è utile aggiornare l'intera governance privacy, introducendo informative più leggere quando le condizioni lo consentono, gestendo con maggiore precisione gli abusi nell'esercizio dei diritti e adottando i nuovi modelli europei per le DPIA. La gestione degli incidenti richiede un approccio più focalizzato perché la soglia di rischio alta diventa il nuovo criterio per la notifica e il termine si estende a 96 ore con obbligo di utilizzare il Single Entry Point non appena sarà attivato.

Un altro ambito cruciale riguarda i cookie e le tecnologie similari. Occorre infatti cominciare a preparare gli ambienti web e app alla futura introduzione dei segnali automatici di scelta che i browser e le wallet europee dovranno supportare. Per alcune categorie di operatori, come i media service provider, la disciplina sarà più flessibile ma tutti dovranno ripensare l'interfaccia di consenso in modo coerente con il nuovo articolo 88a del GDPR.

Sul fronte della sicurezza informatica è importante predisporre per tempo le procedure interne che accompagneranno l'uso del Single Entry Point. Questo implica disegnare flussi chiari tra IT, sicurezza, risk management e privacy, assicurando che i dati richiesti dai template europei siano raccolti in modo coerente e facilmente richiamabile. In caso di indisponibilità tecnica del portale occorrerà mantenere pronti canali alternativi nazionali.

Per quanto riguarda il riuso dei dati pubblici, le amministrazioni dovranno adottare licenze standard, aggiornare i cataloghi degli high value datasets e assicurare modalità di accesso semplici e non discriminatorie. Le imprese che intendono richiedere dati alla PA dovranno invece predisporre procedure che rispettino il nuovo assetto limitato alle emergenze pubbliche e garantiscano tutela effettiva dei segreti commerciali.

Lo sviluppo e l'utilizzo di sistemi di intelligenza artificiale richiederanno una documentazione più attenta delle basi giuridiche utilizzate, soprattutto quando si fa ricorso al legittimo interesse nell'addestramento dei modelli. Occorrerà inoltre gestire con prudenza le eventuali presenze residuali di categorie particolari di dati, scegliendo tecniche di protezione adeguate e assicurando che la rimozione sia tentata ogni volta che lo sforzo non risulti sproporzionato.

Scadenze e tappe da conoscere

La proposta è stata presentata il 19 novembre 2025. Da quel momento si apre una sequenza temporale che guiderà l'implementazione.

Il Single Entry Point per la notifica degli incidenti, gestito da ENISA, dovrà essere adottato obbligatoriamente entro diciotto mesi dalla data di entrata in vigore del regolamento. La Commissione potrà estendere il termine a ventiquattro mesi qualora le condizioni tecniche lo richiedano. Il portale coprirà NIS2, eIDAS, DORA, GDPR e CER e sostituirà progressivamente i canali nazionali, che resteranno attivi solo in caso di indisponibilità tecnica.

Le nuove regole su cookie e memorizzazione delle informazioni nel terminale saranno integrate nell'articolo 88a del GDPR. Quando lo standard europeo sui segnali di consenso diventerà disponibile, tutti i siti e le applicazioni dovranno adeguarsi entro sei mesi, con l'unica eccezione dei media service provider.

In tema di data breach, la notifica alle autorità nazionali sarà richiesta soltanto quando il rischio per gli interessati è elevato. Il termine massimo sarà di 96 ore e la comunicazione dovrà essere inviata tramite il Single Entry Point utilizzando il modello europeo adottato con atto esecutivo.

Il Data Act subirà rafforzamenti specifici: la condivisione B2G sarà ammessa solo per emergenze pubbliche, saranno previste tutele più forti per i segreti commerciali nei confronti di Paesi terzi, e verranno alleggeriti gli obblighi di switching nei contratti cloud precedenti al 12 settembre 2025. I requisiti obbligatori sugli smart contract saranno abrogati.
L'intero corpus del DGA, dell'FFDR e della Open Data Directive confluirà nel Data Act nei nuovi capitoli VIIa, VIIb e VIIc.

Il Regolamento P2B verrà abrogato, pur mantenendo in vita alcuni richiami presenti in altri atti fino al 31 dicembre 2032.

Sono previste poi le valutazioni periodiche: il Data Act dovrà essere riesaminato entro il 12 settembre 2028 e i nuovi capitoli introdotti dall'Omnibus saranno valutati a cinque anni dall'entrata in vigore.

Cronoprogramma operativo per imprese e PA

Fase 0 – Dall'adozione alla pubblicazione in Gazzetta

Occorre monitorare l'intero iter istituzionale seguendo gli emendamenti proposti da Parlamento e Consiglio e gli atti delegati relativi ai modelli per DPIA, breach e segnali di consenso. È utile svolgere una gap analysis trasversale per comprendere come le nuove norme toccheranno GDPR, Data Act, NIS2, DORA, eIDAS, CER e l'intera gestione del consenso digitale.

Fase 1 – Dalla pubblicazione a tre mesi

Le organizzazioni possono cominciare ad aggiornare le policy privacy, adeguare informative e criteri di accesso al terminale, ridefinire la gestione degli abusi del diritto di accesso e integrare la nuova soglia di rischio per i data breach. È il momento di disegnare il nuovo banner cookie e predisporre l'infrastruttura per i segnali machine readable. In ambito contrattuale è necessario rivedere i contratti IaaS, PaaS, SaaS e i servizi custom made siglati prima del 12 settembre 2025, così da rimuovere clausole incompatibili con il percorso europeo verso l'eliminazione delle egress charges.

Fase 2 – Dal terzo al sesto mese

Si può progettare il collegamento tecnico al Single Entry Point, integrandolo con gli strumenti di gestione delle segnalazioni interne.
I registri dei trattamenti devono riflettere i chiarimenti sull'addestramento dell'intelligenza artificiale e sulle nuove regole per la ricerca. Occorre predisporre controlli specifici per i sistemi biometrici in modalità uno a uno.
Le amministrazioni dovranno migrare i processi di riuso dati al nuovo capitolo VIIc del Data Act mentre le imprese devono prepararsi a rispondere alle richieste B2G solo in caso di emergenze pubbliche.

Fase 3 – Dal sesto al dodicesimo mese

Quando lo standard sui segnali di consenso sarà pubblicato, partire con la pianificazione dell'adeguamento. Sul fronte della protezione dei segreti commerciali occorre introdurre procedure interne che consentano di valutare in modo strutturato il rischio di divulgazione verso terzi e quindi motivare un eventuale rifiuto alla condivisione dei dati.

Fase 4 – Dal dodicesimo al diciottesimo mese

Il Single Entry Point diventa obbligatorio. Tutte le notifiche dovranno transitare da questa piattaforma unificata, mentre i canali alternativi rimarranno attivi solo se motivati

dall'impossibilità tecnica. È utile programmare esercitazioni congiunte tra CISO, DPO e responsabili ICT per verificare che la catena di segnalazione funzioni in modo fluido.

Fase 5 – Oltre i diciotto mesi

Il percorso di adeguamento continua nel tempo. Nel 2028 occorre contribuire alla valutazione del Data Act. A cinque anni dall'entrata in vigore si valuterà l'efficacia dei nuovi capitoli su intermediazione, free flow e riuso dei dati pubblici. Nel 2032 si chiuderanno definitivamente gli effetti residui del Regolamento P2B, per cui i contratti e le policy che ancora lo richiamano dovranno essere aggiornati.

Tabella operativa – Periodo, Attività, Funzioni responsabili, Output attesi

Periodo	Attività chiave (versione discorsiva)	Funzione responsabile	Output atteso (versione discorsiva)
T0 – T0 + 3 mesi	Le strutture interne dedicano le prime settimane all'aggiornamento delle policy privacy e delle procedure per la gestione degli incidenti, allineando informative, flussi di consenso e modelli organizzativi al nuovo quadro europeo. Il lavoro richiede un dialogo costante tra team privacy, legali e digitali affinché anche la user experience di banner e interfacce venga riprogettata in coerenza con il GDPR aggiornato.	DPO + Ufficio Legale + Team Web/App	Un set di informative aggiornate, una procedura di gestione dei data breach conforme al limite delle 96 ore e un sistema di raccolta del consenso già predisposto per accogliere i futuri segnali standardizzati.
T0 – T0 + 6 mesi	Le funzioni di sicurezza e rischio IT progettano l'integrazione tecnica con il Single Entry Point, creando connettori, workflow e runbook che permettono di unificare le segnalazioni richieste dalle diverse normative europee. In parallelo, si realizza un mapping completo tra DORA, NIS2, eIDAS e CER, così che i flussi interni possano essere armonizzati.	CISO + IT Risk	Un sistema GRC e ITSM integrato con il SEP, corredato da un playbook operativo che guida le segnalazioni multi-regime.

Periodo	Attività chiave (versione discorsiva)	Funzione responsabile	Output atteso (versione discorsiva)
T0 – T0 + 6 mesi	Gli uffici contrattuali avviano una revisione sistematica di tutti i contratti cloud, inclusi quelli relativi a servizi fortemente personalizzati. L'obiettivo è individuare clausole incompatibili con la futura eliminazione delle egress charges e con i nuovi obblighi europei sullo switching, predisponendo un piano graduale di adeguamento.	Procurement + IT + Ufficio Legale	Una matrice chiara delle clausole da modificare e un percorso definito per l'aggiornamento o la rinegoziazione dei contratti più critici.
T0 – T0 + 9 mesi	In questa fase prende forma il nuovo quadro interno dedicato all'intelligenza artificiale e alla ricerca. Privacy e AI Lead lavorano insieme per definire policy comuni sull'addestramento dei modelli, sui test e sulle tecniche di protezione, costruendo DPIA condivise e armonizzate con il GDPR e con gli obblighi dell'AI Act.	DPO + AI Lead	Un framework di governance dell'AI che include policy di training, misure tecniche di salvaguardia e modelli di DPIA utilizzabili in modo uniforme.
T0 – T0 + 12 mesi	Le amministrazioni pubbliche aggiornano i processi interni di riuso dei dati, adottando il nuovo capo VIIc del Data Act. Ciò comporta la revisione dei cataloghi, l'adozione di licenze standard e la messa a disposizione degli high value datasets tramite API affidabili e documentate.	Open Data Office / PA	Cataloghi aggiornati, licenze uniformi e un'infrastruttura tecnica che consente un accesso più semplice e chiaro ai dati di interesse pubblico.
T0 + 12 – 18 (24) mesi	Il Single Entry Point entra in esercizio obbligatorio e tutte le notifiche devono transitare da questa piattaforma. Le funzioni di sicurezza e privacy conducono esercitazioni interne per testare la catena di segnalazione e assicurare che l'organizzazione sia pronta a utilizzare il meccanismo "report once share many".	CISO + DPO	Un sistema di incident reporting pienamente operativo e un'organizzazione allenata a gestire notifiche integrate secondo il modello europeo.

Rischi e attenzioni

Nel percorso di attuazione del Digital Omnibus emergono alcuni punti che richiedono particolare cautela. Il primo riguarda gli standard europei per i segnali di consenso. Quando lo standard sarà finalmente pubblicato partirà un conto alla rovescia di sei mesi entro cui siti e applicazioni dovranno adeguarsi. È quindi prudente programmare con anticipo lo sviluppo tecnico e la fase di qualità del nuovo sistema di raccolta del consenso per evitare interventi affrettati o soluzioni instabili.

Un secondo elemento riguarda il riuso dei dati pubblici da parte delle very large enterprises e in generale dei gatekeeper. Le pubbliche amministrazioni avranno la possibilità di applicare condizioni economiche più elevate purché basate su criteri oggettivi. Questo richiede una criteriologia solida e trasparente così da prevenire contenziosi e assicurare che la differenziazione delle fee sia sempre proporzionata e verificabile.

Il terzo punto di attenzione tocca la protezione dei segreti commerciali quando i dati rischiano di fuoriuscire verso giurisdizioni extra UE con tutele insufficienti. La valutazione del rischio elevato dovrà essere accuratamente documentata insieme alle ragioni del rifiuto alla condivisione. Restano previsti canali di reclamo che richiederanno decisioni motivate e coerenti con la normativa per dimostrare che la tutela degli asset industriali è stata gestita con prudenza e rigore.