Cosa può cambiare con il Digital Omnibus?

Premesse

Nell'imminenza della discussione del nuovo quadro europeo sul "Digital Omnibus" è essenziale che le Autorità siano pienamente operative e in dialogo trasparente per affrontare un **periodo cruciale per la difesa dei diritti digitali e dei dati personali dei cittadini europei**.

1. Il **"Digital Package on Simplification" (Digital Omnibus)**, atteso per il fine novembre 2025 segnerà un punto di svolta nella regolamentazione digitale europea. Le riforme toccheranno in profondità, fra l'altro, **GDPR, AI Act, Data Act, E Directive** e l'intero corpus normativo sul digitale.

È dunque indispensabile una **Autorità Garante per la protezione dei dati personali** concentrata sul tema e pienamente costituita, che dialoghi apertamente con la politica e vigili affinché la semplificazione normativa non comprometta i diritti fondamentali.

2. In Italia, il Parlamento dovrà farsi protagonista della revisione del Codice Privacy (D.Lgs. 196/03), oggi frammentato, in parte superato e parzialmente inattuato. In quel contesto i parlamentari potranno discutere e valutare se lo schema di governance dell'Autorità (Autorità vs. Agenzia) resti adeguato al contesto digitale e se non sia necessario e opportuno pensare ad una governance comune per Privacy e AI.

3. Per la funzione del **Data Protection Officer** è ormai indispensabile istituire, presso l'Autorità per la protezione dei dati, un canale di comunicazione e supporto dedicato – come già previsto da altre Autorità europee (CNIL).

Serve una semplificazione strutturale nei rapporti e tempi certi di risposta per le imprese. Le aziende non possono attendere mesi (in alcuni casi più di un anno) per avere riscontro (ed in alcuni casi non avere) su notifiche di data breach o procedimenti sanzionatori.

4. L'Italia rischia di restare ai margini di questo cambiamento europeo se non riuscirà a superare con determinazione la fase di instabilità istituzionale. **È il momento di unire competenze, responsabilità e visione**, perché la riforma digitale in corso rappresenta una sfida decisiva per l'intero sistema Paese. È necessario quindi rafforzare la partecipazione attiva dell'Italia nei consessi europei di coordinamento. Una presenza autorevole è essenziale affinché le esigenze dei nostri associati siano rappresentate nel processo decisionale europeo" prima del testo attuale

Introduzione

La proposta di riforma contenuta nel **Digital Omnibus Package della Commissione Europea** (settembre 2025) rappresenta il più ampio intervento di revisione del quadro digitale europeo dopo l'entrata in vigore del GDPR.

L'obiettivo dichiarato è quello di semplificare e armonizzare la normativa sulla protezione dei dati, riducendo gli oneri amministrativi per le imprese e garantendo maggiore coerenza con gli altri regolamenti europei in materia di **AI Act, NIS2, Data Governance Act, ePrivacy ed EIDAS 2**.

Pur non modificando formalmente la struttura del GDPR, il pacchetto introduce interventi selettivi ma sostanziali su alcuni articoli chiave, che incidono in modo

significativo sull'equilibrio originario fra tutela dei diritti fondamentali e flessibilità operativa per titolari e responsabili del trattamento.

Complessivamente, la riforma tende a razionalizzare e integrare il sistema di compliance, ma anche a ridurre la granularità della tutela prevista dal GDPR del 2016, spostando l'asse dalla protezione individuale alla gestione del rischio digitale.

Le osservazioni personali che seguono forniscono una lettura comparata articolo per articolo, evidenziando le principali differenze, i potenziali impatti applicativi e i rischi interpretativi connessi alle nuove formulazioni.

GDPR

1. Articolo 4 – Definizioni

- **Novità:** introduzione del concetto di "**personal data**" relativo ***solo rispetto al soggetto che può ragionevolmente identificare l'interessato*** ("subjective approach").
- **Effetto:** dati che non consentono a un ente di identificare una persona non sarebbero personali *per quell'ente*.
- **Rischio:** si restringe notevolmente l'ambito di applicazione del GDPR; possibile conflitto con l'art. 8 della Carta UE.

2. Articolo 9 – Dati particolari

- **Modifica:** la protezione si applica solo a dati che "rivelano **direttamente**" l'informazione sensibile.
- **Esclusi:** dati che la rivelano solo per deduzione o correlazione.
- **Aggiunta:** nuova deroga (punto k) per uso di dati sensibili nello *sviluppo e funzionamento di sistemi di IA*, se la rimozione è "disproporzionata".

- **Effetto:** significativa riduzione della tutela per inferenze e profilazioni; ampia "licenza" per l'uso in AI training.

3. Articolo 12 – Esercizio dei diritti

- **Novità:** il diritto d'accesso può essere negato o soggetto a un contributo se "abusivo" o "utilizzato per scopi diversi dalla tutela dei dati".
- **Effetto:** possibile restrizione del diritto di accesso ex art. 15 GDPR, con rischio di abuso da parte dei Titolari del trattamento ed inversione dell'onere della prova.

4. Articolo 13 – Informativa

- **Estensione dell'esenzione:** non obbligatoria se esiste un "**rapporto chiaro e circoscritto**" (es. artigiano/cliente) e l'attività "**non è data-intensive**".
- **Effetto:** ampia discrezionalità e minore trasparenza; l'informativa completa diventerebbe necessaria solo per trattamenti complessi o ad alto rischio.

5. Articolo 22 – Decisioni automatizzate e profilazione

- **Modifica:** l'uso di decisioni completamente automatizzate è ammesso anche se la stessa decisione *potrebbe* essere presa da un umano.
- **Effetto:** eliminato il principio di necessità; apre all'uso generalizzato di algoritmi per decisioni contrattuali o selezioni.

Nuovo testo proposto nel Digital Omnibus (bozza 2025)

1. L'interessato ha il diritto di non essere soggetto a una decisione che si basi unicamente o principalmente su un trattamento automatizzato, inclusa la profilazione, qualora tale decisione produca effetti giuridici significativi e non siano previste garanzie adeguate.

2. È consentito l'uso di processi decisionali automatizzati quando:

a) **la decisione è ragionevolmente equivalente a una decisione che un operatore umano avrebbe potuto adottare**;

b) la decisione è necessaria per la prestazione di un servizio o per l'esecuzione di un contratto, purché l'interessato sia adeguatamente informato;

c) **la decisione è conforme ai principi dell'AI Act e ai codici di condotta riconosciuti**.

3. **L'intervento umano deve essere effettivo e proporzionato rispetto alla natura del processo, ma non è richiesto quando la decisione è "assistita da AI conforme" e soggetta a controllo di affidabilità e audit ex AI Act**.

4. La Commissione, mediante atti delegati, può adottare linee guida tecniche per determinare le categorie di trattamenti che rientrano o sono esclusi dal presente articolo.

6. Articolo 30 – Registro dei trattamenti

Novità di questo documento nel **pacchetto Digital Omnibus 2025** versione novembre '25 - (Call for Evidence EC_1762585051 e Draft Changes to GDPR and ePrivacy v1.0):
👉 **non è prevista alcuna modifica diretta o riscrittura dell'articolo 30 del GDPR** ("Registri delle attività di trattamento").

Tuttavia, il documento prevede **modifiche indirette** che **ne riducono di fatto la portata e gli obblighi**, attraverso tre canali normativi collegati.

7. Articolo 33 – Data breach

- **Soglia di notifica:** da "rischio" a "**alto rischio**" per i diritti e le libertà.
- **Tempo di notifica:** da 72 a 96 ore.
- **A chi notificare?** Single-entry point – quindi potrebbe passare tutto ad ACN
- **Effetto:** drastica riduzione delle notifiche ai Garanti; minore controllo e trasparenza.

Nuovo testo proposto nel "Digital Omnibus"

1. In caso di violazione dei dati personali che è suscettibile di comportare un rischio elevato (**high risk**) per i diritti e le libertà delle persone fisiche, **il Titolare notifica senza indebito ritardo e, ove possibile, entro 96 ore, tramite lo sportello unico ("single-entry point")** previsto dall'art. 23a della Direttiva NIS2, all'autorità di controllo competente.

1a. Fino all'istituzione del single-entry point, i titolari notificano direttamente alle autorità nazionali competenti.

6–7. L'EDPB predispone e trasmette alla Commissione un modello comune di notifica (template) e una metodologia uniforme; la Commissione può adottare il modello mediante atto di esecuzione e aggiornarlo ogni tre anni.

8. Articolo 35 – Valutazione d'impatto (DPIA)

- **Centralizzazione:** le liste delle operazioni soggette o escluse da DPIA passano dalle autorità nazionali al **Comitato europeo (EDPB)** e alla Commissione.
- **Effetto:** maggiore armonizzazione, ma riduzione del margine di autonomia delle autorità nazionali.

Il testo della bozza europea **modifica soprattutto i paragrafi 1, 3, 4 e 10**, introducendo questi concetti chiave:

1. Il titolare del trattamento effettua una valutazione d'impatto quando un tipo di trattamento, considerata la natura, l'ambito e le tecnologie utilizzate, **può presentare un rischio elevato non adeguatamente mitigato per i diritti e le libertà delle persone**.

3. La Commissione e il Comitato europeo per la protezione dei dati (EDPB) stabiliscono e aggiornano un elenco comune di trattamenti per i quali è richiesta o non è richiesta una DPIA.

4. Le autorità nazionali non pubblicano più elenchi autonomi, ma possono proporre aggiornamenti all'elenco comune tramite l'EDPB.

7. La DPIA può essere redatta secondo un modello standard europeo, approvato dalla Commissione mediante atti di esecuzione.

10. La consultazione preventiva dell'Autorità è necessaria solo se la DPIA rientra tra i casi definiti come "**ad alto rischio sistemico**" nell'elenco europeo o se il trattamento riguarda sistemi di IA ad alto rischio ai sensi dell'AI Act.

9. Articolo 41a – Pseudonimizzazione

- **Placeholder:** consente alla Commissione di definire con atti delegati cosa è "pseudonimizzazione".
- **Effetto:** possibilità di ridefinire in futuro l'ambito dei dati personali → rischio di riduzione della tutela via atti tecnici.

10. Articolo 57 – Sandbox regolatori

- **Nuovo compito dei Garanti:** creare "regulatory sandboxes" per testare tecniche e soluzioni.
- **Effetto:** utile all'innovazione, ma serve chiarire limiti e garanzie per i diritti degli interessati.

E-Directive e GDPR

Articolo 88a – Trattamento su terminali (nuovo)

- **Trasferimento di regole da ePrivacy a GDPR.**
- **Autorizza trattamenti "on or from" dispositivi (smartphone, PC, TV)** per finalità specifiche (trasmissione, servizio richiesto, sicurezza, misurazione audience).
- **Effetto:** sostituisce l'attuale art. 5(3) ePrivacy (**cookie law**) → **riduzione della protezione dei dispositivi e rischio di sorveglianza estesa**.

L'articolo **88a** della proposta di riforma ("**Digital Omnibus**") rappresenta **uno dei punti più delicati** e innovativi, poiché **sposta parte della disciplina della Direttiva ePrivacy (art. 5, par. 3)** all'interno del **GDPR**, modificando profondamente il regime dei cosiddetti *cookie e tecnologie di tracciamento*.

1. Contesto normativo

L'art. 5(3) della Direttiva ePrivacy (2002/58/CE) stabilisce oggi che:

"È consentito l'immagazzinamento di informazioni o l'accesso a informazioni già archiviate nel terminale dell'utente solo se l'utente ha espresso il suo consenso, salvo che tali operazioni siano strettamente necessarie per fornire un servizio richiesto."

Il nuovo **art. 88a GDPR** mira a **integrare e sostituire** in parte questa norma, unificando nel GDPR la disciplina sul trattamento dei dati *"on or from terminal equipment"*.

2. Struttura e contenuto del nuovo articolo 88a

Comma 1 – Trattamenti consentiti senza consenso

Il trattamento dei dati personali "sul o dal terminale" è lecito **solo se strettamente necessario** per:
a) trasmissione di comunicazioni elettroniche;
b) fornitura di un servizio esplicitamente richiesto dall'interessato;
c) creazione di statistiche aggregate sull'uso di un servizio online per finalità di misurazione dell'audience (solo uso interno del titolare);
d) mantenimento o ripristino della sicurezza del servizio o del terminale.

Nota: queste quattro ipotesi equivalgono alle "eccezioni al consenso" oggi riconosciute per cookie tecnici e di sicurezza, ma con un ambito potenzialmente più ampio.

Comma 2 – Trattamenti basati su consenso

Se il trattamento si fonda su **art. 6(1)(a) GDPR (consenso)**:

- L'utente deve poter **dare o rifiutare** il consenso in modo **"facile e comprensibile"**, con un **"single-click button o equivalente"**;
- La scelta (rifiuto o accettazione) deve essere **rispettata per almeno 6 mesi**, senza nuove richieste per lo stesso scopo.

Conseguenza: si tenta di ridurre la "**consent fatigue**", ma si introduce l'obbligo di *memorizzare* la scelta (quindi un tracciamento minimo resta inevitabile).

Comma 3 – Trattamento per marketing basato su legittimo interesse

Se il trattamento si basa su **art. 6(1)(f)** per finalità di *marketing diretto*, l'utente deve poter esercitare **l'opposizione (opt-out)** con un clic (**"single-click button**").

Ciò apre alla possibilità di **profilazione pubblicitaria senza consenso**, fondata su legittimo interesse, purché vi sia un meccanismo di opposizione semplificato.

3. Recital 37 e 38 – Logica dichiarata del legislatore

Il legislatore giustifica la norma sostenendo che:

- occorre "unificare" la disciplina GDPR/ePrivacy,
- ridurre gli oneri per i titolari del trattamento,
- semplificare il quadro per i trattamenti "a basso rischio".

In particolare, si sottolinea che:

il GDPR deve diventare l'unico regime giuridico per i trattamenti di dati personali effettuati "sul o dal terminale".

Criticità principali

a) Estensione del perimetro

Il testo parla di dati trattati **"on or from terminal equipment"**, non solo "stored or accessed".
Quindi copre **qualsiasi trattamento di dati personali tramite dispositivi** (smartphone, PC, smart TV, IoT).
Non si limita al deposito di cookie, ma include ogni forma di elaborazione locale o remota originata dal dispositivo.

b) Rischio di indebolimento della protezione dei dispositivi

L'art. 5(3) ePrivacy tutela non solo la privacy, ma anche **l'integrità del terminale**.
Trasferendo la materia al GDPR, tale protezione "tecnica" si perde, riducendo la barriera contro accessi non autorizzati o sorveglianza dei device.

c) Moltiplicazione delle basi giuridiche

Combinando le ipotesi del par. 1 (a-d) con le basi dell'art. 6 e 9 GDPR, si ottengono **oltre 10 possibili basi legali**.
I titolari avranno ampia discrezionalità nel giustificare i trattamenti, con rischio di **forum shopping** giuridico.

d) Ambiguità del "legittimo interesse"

Il riferimento all'art. 6(1)(f) per il marketing riapre la possibilità di tracciamento senza consenso, contrastando la giurisprudenza (es. *Planet49*, C-673/17).

e) Ambiguità del "single-click button"

Non vengono definiti standard tecnici.
Consentirà di continuare con *dark patterns* (pulsanti diseguali, opzioni nascoste) che già le Autorità Garanti Privacy considerano pratiche scorrette.

f) AI e profilazione

I dati **"on or from devices"** potranno essere facilmente riutilizzati per **addestrare sistemi di IA** (anche con base di legittimo interesse), specialmente considerando l'art. 9(2)(k) proposto → **circolo vizioso fra device data e AI training**.

Cybersecurity / NIS2

- Integrazione del sistema di **incident reporting** tra GDPR, NIS2 e altri regolamenti settoriali (DORA, EHDS).
- Creazione di un **"single-entry point"** nazionale per tutte le notifiche (data breach, incidenti cyber, IA).

- Adozione di un **modello unico di notifica UE** (template e metodologia comuni).

- Obiettivo: armonizzazione; rischio: perdita di specializzazione privacy e minore tempestività.
- Per l'Italia il "**single – entry point**" potrebbe essere **ACN**

AI Act

- Misure di "applicazione semplificata" per PMI e medie imprese (*mid-caps*).
- Allineamento dei regimi di *reporting*, *registrazione* e *monitoraggio* con GDPR e NIS2.
- Possibilità di usare dati sensibili nel training di sistemi di AI in deroga all'art. 9, se la rimozione è "sproporzionata".
  Effetto: semplificazione per fornitori AI, ma rischio di attenuazione dei limiti etici e privacy-by-design.

Rapporti giornalistici (Financial Time) indicano che la European Commission sta valutando un "**grace period**" di circa un anno per alcune parti del testo, in particolare per i modelli generali e gli obblighi più gravosi, in vista del pacchetto "digital omnibus".

EIDAS 2 (European Digital Identity Framework)

Il Digital Omnibus interviene su EIDAS 2 razionalizzando gli obblighi per i trust service providers e raccordando l'identità digitale con gli altri pilastri del diritto digitale UE (GDPR, NIS2, AI Act, Data Governance Act).

Introduce e valorizza il concetto di EU Digital Identity / Business Wallet, **estendendo l'identità digitale anche alle persone giuridiche per firme, sigilli, deleghe e accessi certificati in tutta l'Unione**.

L'obiettivo è ridurre costi e duplicazioni di certificazioni, creando un'unica infrastruttura di fiducia europea, con il rovescio della medaglia di una maggiore centralizzazione delle credenziali digitali e dei relativi rischi di sicurezza e concentrazione del potere informativo.

Fonti principale:

- Documento originale *Draft Changes to GDPR and ePrivacy – Comparison Comments* (noyb v1.0) e Call for Evidence EC_1762585051

- Digital Omnibus – Call for Evidence, Ref. Ares(2025)7724296 del 16/09/2025 e Draft Changes to GDPR and ePrivacy – v1.0

Elaborazione a fini divulgativi e di studio, redatta sulla base delle bozze e dei documenti disponibili al momento della pubblicazione.
Il contenuto non ha carattere esaustivo né valore ufficiale e ***potrebbe essere oggetto di aggiornamenti o superato da versioni successive delle proposte legislative*** *in corso di adozione da parte della Commissione europea o del Parlamento europeo.*
Le valutazioni e i commenti riportati riflettono esclusivamente un'interpretazione tecnica e comparata, a supporto dell'approfondimento professionale e accademico in materia di diritto della protezione dei dati e governance dell'intelligenza artificiale.