CONFINDUSTRIA

Digital Package: le modifiche al GDPR nella proposta di Regolamento Omnibus Digitale

Nota di Aggiornamento

2 dicembre 2025

Sommario

1. Premessa

Il 19 novembre scorso, la Commissione europea ha presentato il c.d. **Digital Package**[1], un insieme di iniziative volte a creare un ecosistema digitale europeo più semplice e favorevole all'innovazione e alla competitività delle imprese.

Il pacchetto comprende tre interventi principali:

1. la **proposta di Regolamento c.d. Omnibus Digitale**[2] (di seguito, anche "**Proposta**" o "**Omnibus Digitale**"), che modifica nove atti legislativi in materia di dati, tecnologie digitali, intelligenza artificiale (IA) e cibersicurezza, con l'obiettivo di ridurre gli oneri a carico delle imprese e favorire la disponibilità e l'utilizzo dei dati.

   In particolare, la Proposta modifica: ***i)*** il Regolamento UE n. 679/2026, c.d. **GDPR**; ***ii)*** la Direttiva n. 58/2002, c.d. **e-Privacy**; ***iii)*** il Regolamento UE n. 1725/2018 sul trattamento dei dati personali da parte delle Istituzioni UE; ***iv)*** il Regolamento UE n. 2854/2023, c.d. *Data Act*; ***v)*** il Regolamento UE n. 1724/201, c.d. *Single Digital Gateway* (SDG); ***vi)*** la Direttiva n. 2555/2022, c.d. NIS 2; ***vii)*** il Regolamento UE n. 910/2014, c.d. e-IDAS; ***viii)*** il Regolamento UE n. 2554/2022, c.d. *Digital Operational Resilience Act* (DORA); ***ix)*** la Direttiva n. 2557/2022;

2. la nuova Strategia dell'Unione europea dei dati, c.d. **EU Data Union Strategy**[3], che mira a: ***i)*** aumentare l'accesso ai dati per lo sviluppo dell'IA e garantire alle imprese la disponibilità di informazioni di alta qualità necessarie per l'innovazione. A tal fine, si prevede l'avvio dei primi *data labs* europei, strutture pubblico-private, che collegheranno gli spazi di dati ai diversi ecosistemi di IA e metteranno a disposizione *dataset* settoriali di alta qualità per imprese, comprese le PMI, e ricercatori che utilizzano l'IA. Parallelamente, la Strategia prevede di ampliare gli *European Data Spaces* e di rafforzare gli strumenti trasversali della *data economy*, promuovendo tra l'altro l'uso di dati sintetici; ***ii)*** razionalizzare le norme sui dati per garantire certezza del diritto e ridurre i costi di conformità; ***iii)*** salvaguardare la sovranità dell'UE in materia di dati e rafforzare la posizione globale dell'UE sui flussi internazionali di dati. Al riguardo, si prevede l'adozione di orientamenti sul trattamento equo dei dati dell'UE all'estero, per fornire criteri chiari alle imprese e alle autorità, nonché di un *toolbox anti-leakage* per contrastare la localizzazione ingiustificata, le misure discriminatorie, le esclusioni arbitrarie e il rischio di perdita di dati sensibili non personali;

3. la proposta di Regolamento che istituisce il portafoglio europeo delle imprese, c.d. **European Business Wallet**[4], che consentirà agli operatori di identificare, autenticare e scambiare in modo sicuro i dati nell'UE.

---

[1] V. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2718.

[2] V. https://digital-strategy.ec.europa.eu/it/library/digital-omnibus-regulation-proposal.

[3] V. https://digital-strategy.ec.europa.eu/en/policies/data-union.

[4] V. https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-establishment-european-business-wallets.

Il Digital Package riconosce il valore che i dati - personali e non personali - generano nell'economia digitale dell'UE e l'esigenza di agevolarne l'utilizzo da parte delle imprese europee, puntando ad assicurare certezza e coerenza all'*acquis* legislativo, ridurre gli oneri di conformità e sostenere l'implementazione e l'uso responsabile dell'IA.

In tale contesto, l'Omnibus Digitale dispone **modifiche alla normativa sulla protezione dei dati personali**.

In particolare, come riportato nella Relazione illustrativa, la Proposta risponde alle preoccupazioni sollevate dalle imprese in merito alle difficoltà riscontrate nell'applicazione del GDPR e mira a:

- aggiornare e chiarire alcuni aspetti della normativa in materia di dati personali (es. utilizzo dei dati pseudonimi, definizione di ricerca scientifica);
- semplificare l'adempimento di alcuni obblighi particolarmente gravosi (es. valutazione d'impatto sulla protezione dei dati, c.d. DPIA, notifica delle violazioni dei dati personali, c.d. *data breach*);
- favorire l'utilizzo dei dati personali per lo sviluppo di sistemi e modelli di IA responsabile

In generale, le modifiche proposte sono condivisibili e intervengono su questioni rilevanti, segnalate in più occasioni anche da Confindustria.

La Proposta seguirà l'*iter* legislativo ordinario e, pertanto, sarà sottoposta all'approvazione del Parlamento europeo e del Consiglio dell'UE.

Di seguito, una sintesi delle modifiche proposte dall'Omnibus Digitale alla normativa sulla protezione dei dati personali di rilevanza per le imprese.

2. Modifiche al GDPR

Come anticipato, l'Omnibus Digitale contiene una serie di modifiche al GDPR.

Tra gli interventi di maggiore interesse per le imprese, si segnalano:

1. la **modifica della definizione di "dato personale"** (art. 4, par. 1, n. 1 del GDPR).

   In linea con quanto stabilito dalla Corte di Giustizia dell'UE, nella sentenza 4 settembre 2025 - causa C-413/23[5], la nozione assume una **dimensione soggettiva**, variando in base al soggetto che detiene le informazioni e alla sua capacità di riferirle a una persona fisica.

   In particolare, si precisa che un'informazione non è considerata dato personale per un determinato soggetto quando quest'ultimo non dispone di mezzi ragionevolmente utilizzabili per identificare la persona fisica cui l'informazione si riferisce. Pertanto, le informazioni relative a una persona fisica costituiscono dati personali **solo per chi è effettivamente in grado di identificarla**.

[5] V. https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:62023CJ0413.

La modifica incide principalmente sul **trattamento dei c.d. dati pseudonimizzati**[6]. La circostanza che un determinato soggetto sia in grado di identificare una persona fisica non implica, di per sé, che i dati pseudonimizzati debbano essere considerati, in ogni caso e per qualsiasi soggetto, come dati personali tali da determinare l'applicazione del GDPR. Ne consegue che, al fine di stabilire se una persona fisica sia identificabile, occorre considerare i mezzi, ragionevolmente probabili, che possano essere utilizzati per identificarla, direttamente o indirettamente (Considerando n. 27 dell'Omnibus Digitale);

2. l'**introduzione di una definizione di "ricerca scientifica"** (nuovo art. 4, par. 1, n. 38 del GDPR).

   La nuova nozione ricomprende qualsiasi attività di ricerca che possa anche sostenere l'innovazione, come lo sviluppo tecnologico e la sperimentazione. Al riguardo, si specifica che tali attività devono: ***i)*** contribuire alla conoscenza scientifica esistente ovvero applicare in modo nuovo conoscenze già acquisite; ***ii)*** essere svolte con l'obiettivo di accrescere il patrimonio generale di conoscenze e il benessere della società; ***iii)*** rispettare gli standard etici del pertinente settore di ricerca. Inoltre, si precisa che la **ricerca scientifica può avere finalità commerciali**.

   L'intervento è senz'altro positivo, in quanto riconosce in modo esplicito il ruolo delle imprese nella crescita delle conoscenze e nel benessere della società, rendendo più chiari i confini di liceità dei trattamenti di dati personali effettuati per finalità di ricerca scientifica. A tal fine, infatti, ciò che risulta determinante è **l'approccio metodologico e sistematico adottato** e non l'ambito in cui la ricerca o lo sviluppo tecnologico vengono condotti, potendo essere svolti in contesti accademici, ***industriali*** o ***in altri ambienti, comprese le piccole e medie imprese*** (Considerando n. 28 dell'Omnibus Digitale).

   Inoltre, al Considerando n. 32, la Proposta prevede **il trattamento dei dati personali per finalità di ricerca scientifica persegue un interesse legittimo del titolare**, a condizione che la ricerca non sia contraria al diritto UE o nazionale e siano rispettate tutte le altre condizioni previste dall'art. 6, par. 1, lett. f) del GDPR (bilanciamento di interessi), nonché di tutti gli ulteriori requisiti e principi stabiliti dal GDPR;

3. la **modifica del c.d. principio di limitazione della finalità** (art. 5, par. 1, lett. b) del GDPR).

   Con riferimento, tra l'altro, al **trattamento ulteriore per finalità di ricerca scientifica**, si prevede che esso è considerato compatibile con le finalità iniziali, **indipendentemente dalle condizioni dell'art. 6, par. 4 del GDPR** e, dunque, senza la necessità di verificare preliminarmente la compatibilità del trattamento ulteriore in base al nesso tra le finalità originarie e quelle ulteriori, al contesto in cui i dati sono raccolti, alla natura dei dati, alle conseguenze del trattamento ulteriore trattamento e all'esistenza di garanzie adeguate;

---

[6] V. art. 4, par. 1, n. 5 del GDPR: "pseudonimizzazione": il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

4. l'**introduzione di nuove deroghe per il trattamento di categorie particolari di dati personali**, per:

   - **lo sviluppo e il funzionamento di un sistema o di un modello di IA** (nuovo art. 9, par. 2, lett. k) del GDPR).

     Partendo dal presupposto che lo sviluppo dei sistemi e dei modelli di IA comporta la raccolta di grandi quantità di dati, inclusi dati personali e categorie particolari di dati personali, la misura mira a evitare di ostacolare in modo sproporzionato lo sviluppo e il funzionamento dell'IA (Considerando n. 33 dell'Omnibus Digitale).

     Ad ogni modo, la nuova deroga opera **solo se il trattamento di categorie particolari di dati è involontario e residuale**. Di regola, infatti, il titolare è tenuto ad adottare adeguate misure tecniche e organizzative per evitare la raccolta e l'utilizzo di dati "sensibili" nei *dataset* impiegati per addestrare, testare o validare sistemi e modelli di IA, nonché a rimuovere quelli che, nonostante tali accorgimenti, vi confluiscano. Solo qualora la rimozione richieda uno sforzo sproporzionato - in particolare, quando comporterebbe la necessità di riprogettare il sistema o il modello di IA -, il trattamento è ammesso a condizione che il titolare protegga efficacemente tali dati e ne impedisca l'uso per generare *output*, nonché la loro divulgazione o il loro accesso da parte di terzi.

     In tutti gli altri casi, vale a dire quando il trattamento di categorie particolari di dati non è involontario e residuale, ma necessario allo scopo della ricerca, dello sviluppo o del funzionamento del sistema di IA, continua ad applicarsi quanto previsto dall'art. 9, par. 2, lettere da a) a j) del GDPR (Considerando n. 33 dell'Omnibus Digitale);

   - la **verifica biometrica dell'identità decentralizzata** (nuovo art. 9, par. 2, lett. l) del GDPR).

     In particolare, il trattamento di dati biometrici per la verifica dell'identità decentralizzata viene consentito a condizione che il dato biometrico o il mezzo di verifica rimanga sotto il controllo esclusivo dell'interessato. È il caso, a esempio, dei dati biometrici conservati in modo sicuro esclusivamente presso l'interessato, oppure in forma crittografata presso il titolare, ma con la chiave crittografica detenuta unicamente dall'interessato. In tali ipotesti, come previsto dal Considerando n. 34 dell'Omnibus Digitale, il trattamento non è suscettibile di creare rischi significativi per i suoi diritti e le sue libertà fondamentali (il titolare non viene a conoscenza dei dati biometrici o vi accede solo per un periodo molto limitato durante il processo di verifica;

5. la **modifica delle circostanze che consentono di derogare all'obbligo di informativa** (art. 13, par. 4 e 5 del GDPR).

   In particolare, per ridurre ulteriormente gli oneri a carico dei titolari, senza compromettere la possibilità per l'interessato di esercitare i propri diritti, si introduce una deroga all'obbligo di informativa per i trattamenti effettuati nell'ambito di un **rapporto chiaro e circoscritto tra l'interessato e il titolare**, a condizione che essi **non siano intensivi** (riguardino cioè una ridotta quantità di dati personali e comportino operazioni non complesse), **non comportino un rischio elevato** e sussistano motivi ragionevoli per presumere che **l'interessato disponga già delle informazioni** sul titolare, sulle finalità e sulla base giuridica del trattamento (es. trattamento necessario all'esecuzione di un contratto di cui l'interessato è parte o effettuato sulla base del consenso dell'interessato).

Su punto, il Considerando n. 36 dell'Omnibus digitale **esclude espressamente che i trattamenti effettuati in ambito lavorativo possano, di regola, qualificarsi come a bassa intensità e, di conseguenza, beneficiare della nuova deroga**.

Viene, altresì, **confermata la deroga vigente per i trattamenti effettuati per finalità di ricerca scientifica**, nei casi in cui fornire l'informativa risulti impossibile, comporti uno sforzo sproporzionato ovvero rischi di rendere impossibile o compromettere seriamente il conseguimento degli obiettivi del trattamento. Sul punto, il Considerando n. 37 dell'Omnibus Digitale precisa che la fornitura dell'informativa può comportare uno sforzo sproporzionato, in particolare, quando, **al momento della raccolta dei dati, il titolare non sapeva, né prevedeva che li avrebbe trattati successivamente per finalità di ricerca scientifica** e, quindi, potrebbe non disporre facilmente dei dati di contatto degli interessati. In tali situazioni, il titolare dovrebbe informare gli interessati in modo indiretto, ad esempio, rendendo pubblicamente disponibili le informazioni, con modalità idonee a raggiungere il maggior numero possibile di interessati. I mezzi appropriati devono essere individuati in base al contesto del progetto di ricerca e alle categorie di interessati coinvolti;

6. la **modifica alla disciplina del processo decisionale basato unicamente su un trattamento automatizzato** (art. 22 del GDPR).

   In particolare, si prevede che, ai fini dell'instaurazione o dell'esecuzione di un contratto tra l'interessato e il titolare, quest'ultimo possa assumere decisioni basate esclusivamente su un trattamento automatizzato, indipendentemente dal fatto che la medesima decisione possa essere adottata anche mediante intervento umano. In altre parole, il fatto che la decisione potrebbe essere presa anche da una persona fisica non impedisce al titolare di adottarla in via esclusivamente automatizzata. Ad ogni modo, quando esistono più soluzioni di trattamento automatizzato ugualmente efficaci, il titolare dovrebbe utilizzare quella meno invasiva (Considerando n. 38 dell'Omnibus Digitale);

7. le **semplificazioni per le attività di notifica dei *data breach*** (art. 33 del GDPR).

   In particolare, l'obbligo di notifica dei *data breach* al Garante privacy viene circoscritto alle sole violazioni dei dati personali suscettibili di comportare un rischio elevato per i diritti e le libertà delle persone fisiche. Inoltre, il termine per la notifica viene esteso da 72 a 96 ore e, ai fini della notifica, si prevede l'impiego di un punto di accesso unico, che la stessa Proposta istituisce in capo all'Agenzia dell'Unione europea per la cibersicurezza, c.d. ENISA (nuovo art. 23a della Direttiva NIS 2). Resta fermo l'obbligo di documentare la violazione *ex* art. 3, par. 5 del GDPR, nonché quello generale di dimostrare la conformità alla disciplina sulla protezione dei dati personali *ex* art. 5, par. 2 del GDPR (Considerando n. 39 dell'Omnibus Digitale).

   Inoltre, per agevolare il rispetto degli obblighi da parte dei titolari e garantire un approccio armonizzato nell'UE, si prevede la predisposizione, da parte dell'EDPB, di un modello comune di notifica e di un elenco delle circostanze in cui una violazione dei dati personali è suscettibile di comportare un rischio elevato per i diritti e le libertà di una persona fisica;

8. le **semplificazioni per l'esecuzione della DPIA** per i trattamenti suscettibili di comportare un rischio elevato per i diritti e le libertà delle persone fisiche (art. 35 del GDPR).

In particolare, l'elaborazione degli elenchi dei trattamenti soggetti ed esenti all'obbligo di DPIA, oggi affidata alle Autorità di controllo (in Italia, il Garante privacy), viene attribuita all'EDPB. Inoltre, per agevolare lo svolgimento della DPIA, quest'ultimo è incaricato di predisporre un modello comune e di una metodologia comune. La modifica è senz'altro positiva, considerato che l'esecuzione della DPIA costituisce, ad oggi, uno degli adempimenti più complessi, specie per le piccole e medie imprese;

9. l'**introduzione di una disciplina specifica per il trattamento di dati personali nel contesto dello sviluppo e del funzionamento di sistemi e modelli di IA** (nuovo art. 88c del GDPR).

   In tale ambito, il perseguimento del **legittimo interesse** del titolare, ai sensi dell'art. 6, par. 1, lett. f) del GDPR, è individuato come **base giuridica del trattamento**, ove appropriato e purché il trattamento non sia esplicitamente subordinato al consenso dal diritto UE o nazionale.

   In ogni caso, il titolare è tenuto ad adottare adeguate misure organizzative e tecniche, nonché idonee garanzie a tutela dei diritti e delle libertà degli interessati (es. applicazione del principio di minimizzazione nella selezione delle fonti e nelle fasi di addestramento e *test* del sistema o modello di IA; trasparenza rafforzata nei confronti degli interessati; riconoscimento di un diritto incondizionato di opposizione al trattamento all'interessato).

A completamento di questi interventi, l'Omnibus Digitale modifica anche la **Direttiva e-Privacy**, riorganizzando **gli obblighi relativi a *cookie* e tracciamento *online*** e trasferendoli nel GDPR.

A tal fine, sono introdotti i nuovi articoli **88a** e **88b**, che disciplinano il **trattamento dei dati personali nelle apparecchiature terminali delle persone fisiche**.

Tra l'altro, le nuove norme:

- subordinano, in via generale, al **consenso dell'interessato** l'archiviazione di dati personali ovvero l'accesso a dati personali già archiviati nell'apparecchiatura terminale di una persona fisica.

  In particolare, si prevede che: ***i)*** l'interessato deve poter rifiutare le richieste di consenso in modo semplice e comprensibile, con un solo *click* o mezzi equivalenti; ***ii)*** se l'interessato presta il consenso, il titolare non può presentarne una nuova richiesta per la stessa finalità; ***iii)*** se l'interessato rifiuta una richiesta di consenso, il titolare non può presentare una nuova richiesta di consenso per la stessa finalità per un periodo di almeno 6 mesi;

- consentono di memorizzare o accedere a dati personali già memorizzati nell'apparecchiatura terminale di una persona fisica **senza consenso** e di trattarli successivamente per creare informazioni aggregate sull'utilizzo di un servizio *online* e misurare l'utenza del servizio a scopi interni;

- prevedono che le preferenze dell'utente debbano poter essere espresse e trasmesse in un formato che i sistemi informatici possano leggere e interpretare automaticamente (c.d. formato *machine-readable*).