Comunicato Ufficiale in merito alla

Riforma del Regolamento UE 2016/679 (“GDPR”)

Il 19 novembre 2025 la Commissione europea presenterà nell’ambito del c.d. “*Digital Omnibus*” delle modifiche al Regolamento UE 2016/679 (“GDPR”) e al Regolamento UE 2024/1689. Questo documento ha lo scopo di chiarire la posizione di Privacy Network rispetto a tali propositi e diffondere consapevolezza circa l’operazione di riforma normativa in atto.

A seguito della pubblicazione di una prima bozza di questo documento, numerose voci della società civile si sono sollevate al fine di rilevare i pericoli posti da una riforma così strutturata. Privacy Network, che con il proprio comunicato del 28 maggio 2025 aveva espresso le proprie perplessità rispetto ad una potenziale riforma del GDPR, si unisce a tali contestazioni.

Riteniamo, infatti, che le modifiche proposte invertano sistematicamente la gerarchia tra diritti fondamentali e interessi di mercato. Diversi articoli contraddicono la giurisprudenza consolidata della Corte di Giustizia UE e presentano profili di incompatibilità con gli articoli 7 e 8 della Carta dei Diritti Fondamentali. Parallelamente, il Digital Omnibus introduce emendamenti al Regolamento AI (2024/1689) che, combinati con le modifiche GDPR, creano zone di *non-enforcement* strutturale.

Sebbene Privacy Network rimanga ferma nell'idea di dover promuovere lo sviluppo di un ecosistema digitale all'interno del territorio dell'Unione, è altrettanto forte la richiesta per un intervento che si ponga come un corretto bilanciamento tra tali esigenze e la tutela dei diritti fondamentali, il quale costituisce, a nostro avviso, l'unico mezzo per lo sviluppo di un'Intelligenza Artificiale davvero sicura e rispondente a principi di etica e legalità.

L'intervento attualmente in discussione è, al contrario, un malcelato tentativo di deregolamentazione, che interviene solo parzialmente a favore dello sviluppo di un ecosistema come quello sopra descritto. Molte delle disposizioni introdotte appaiono, piuttosto, come un lasciapassare ai grandi player del settore tecnologico nei confronti dei cittadini e delle cittadine.

A ciò si aggiunge il timore che tale intervento di riforma risulti non in una "riduzione" della complessità, ma in suo mero trasferimento. Laddove ora sussistono regole chiare, enforcement centralizzato e regole di trasparenza obbligatoria, lo scenario futuro rischia di presentare definizioni sovrapposte (dato personale oggettivo vs soggettivo, categorie speciali dirette vs inferite), frammentazione competenze tra DPA e autorità settoriali, ed infine opacità sistemica (no registro esenzioni AI Act, no notifiche sotto-soglia violazioni).

In tale scenario gli operatori responsabili affronteranno comunque un elevato grado di incertezza legale (con i relativi costi che ciò rappresenta), mentre quelli che beneficiano delle barriere all'ingresso poste dalle complessità burocratiche avranno la possibilità di sfruttare maggiori zone grigie. In altri termini, si conferma l'idea per cui tale intervento sia maggiormente orientato alla deregolamentazione che alla semplificazione.

Le nostre richieste

Come società civile chiediamo l'apertura di nuovi tavoli di confronto davanti alle istituzioni europee per discutere le modalità e il merito di eventuali riforme al GDPR e all'AI Act, che siano rivolti ad un migliore bilanciamento dei diritti dei cittadini e delle cittadine con le esigenze di sviluppo economico del settore tecnologico.

Chiediamo altresì ai rappresentanti nazionali presso le istituzioni europee di aprire simili tavoli di confronto a livello nazionale e supportare un intervento in tal senso dinanzi al legislatore unionale.

Privacy Network, 17.11.2025

Si riporta in allegato l'analisi dettagliata delle disposizioni e dei rischi posti ad avviso della scrivente associazione ai diritti e alle libertà dei cittadini.

Analisi delle modifiche proposte

Definizione di dati personali

Modifiche proposte

La bozza presentata dalla Commissione propone una revisione dell'art. 4 del GDPR nel senso di prevedere che i dati assumano la caratteristica di "personali" soltanto nel caso in cui risultino identificabili da parte del soggetto che li tratta tenendo conto dei mezzi che può ragionevolmente utilizzare a tale scopo. I dati, inoltre, non assumono natura di dato personale per l'entità in questione solo perché un eventuale destinatario successivo potrebbe disporre di strumenti idonei a identificare l'interessato.

In aggiunta, la proposta prevede una versione dell'art. 9 del GDPR, che non prevederebbe più il concetto di dati "*idonei a identificare*", ma che "*rivelando direttamente*".

Osservazioni

Tale intervento mira a semplificare la circolazione dei dati personali, escludendo dall'ambito di applicazione della norma alcuni dati e escludendo i dati che non rivelano direttamente informazioni sensibili dal campo di applicazione dell'art. 9.

L'intervento si inserisce nel solco della sentenza C-413/23P EDPS v SRB, che ha introdotto la possibilità di valutare l'identificabilità dei dati personali, tenendo conto della posizione ricoperta dal titolare del trattamento al momento della raccolta, e in concreto e mira a semplificare il quadro normativo. La nuova formulazione, infatti, restringe la stessa definizione di dato personale e introduce un elemento di soggettività nella valutazione, legandola alle capacità tecniche del singolo titolare del trattamento[1].

Per quanto l'interpretazione "soggettiva" del concetto di dato personale possa portare ad una facilitazione nelle attività di trattamento da parte di soggetti di limitate dimensioni, che non dispongono delle capacità computazionali e tecnologiche dei player più avanzati, alcune maggiori precauzioni dovrebbero essere adottate:

1 Si noti, comunque, che l'impostazione proposta potrebbe contrastare con altri procedenti della medesima corte (vedi sentenza C-582/14- "Breyer").

- la clausola che esclude la rilevanza della capacità del terzo destinatario dei dati di re-identificare i dati personali (e, quindi rendere il dato soggettivamente non personale per il primo soggetto, identificabile e, pertanto, personale) potrebbe creare mercati illeciti di dati e pratiche lesive dei diritti degli interessati da parte di *data broker* e player in grado di effettuare ampie operazioni di aggregazione;
- difatti, dietro il ricorso a scarse pratiche di *accountability*, tali soggetti potrebbero deliberatamente separare i dati identificativi da quelli apparentemente non riferibili al soggetto, con l'obiettivo di sottrarre tali trattamenti all'ambito di applicazione del GDPR, pur mantenendo, di fatto, la possibilità di tracciare il comportamento o l'identità del soggetto;
- l'accertamento dell'effettiva identificabilità dei dati personali da parte delle Autorità di controllo potrebbe diventare particolarmente difficoltosa e, pertanto, dovrebbero essere adottate specifiche misure e prescrizioni in merito alla dimostrazione della caratteristica di personalità dei dati trattati.

Queste considerazioni assumono particolare rilievo in relazione alle categorie particolari di dati personali, come quelli relativi alla salute, alle convinzioni politiche, alla vita sessuale, all'orientamento sessuale o all'appartenenza sindacale. L'attuale impostazione dell'art. 9 del GDPR tutela in modo rafforzato tali categorie di dati, riconoscendo che anche informazioni apparentemente neutre possono, attraverso la combinazione di altre informazioni rivelare aspetti profondamente personali e privati degli interessati. Finora, la Corte di giustizia dell'Unione europea (CGUE)[2] ha infatti stabilito che la protezione debba estendersi anche a quei dati dai quali si possano dedurre informazioni sensibili, non solo a quelli che le rivelano esplicitamente.

La proposta della Commissione, tuttavia, sembra voler ribaltare questo principio, introducendo nella definizione l'avverbio "direttamente" e limitando così la tutela ai soli casi in cui tali informazioni siano direttamente rivelate. Una simile precisazione non tiene conto (o non vuole tenere conto) della realtà attuale, in cui grandi piattaforme digitali e imprese sfruttano dati "dedotti" per profilare gli utenti, prevedere i comportamenti e indirizzare pubblicità, veicolare contenuti e tendenze di consumo.

[2] Sentenza del 1° agosto 2022, OT contro Vyriausioji tarnybinės etikos komisija, C-184/20, ECLI:EU:C:2022:601.

Anche nella logica di voler rendere più semplici determinate operazioni sui dati appartenenti a categorie particolari, un intervento legislativo in tal senso dovrebbe concentrarsi sulla modifica o ridefinizione di alcuni degli elementi di legittimità previsti dall'art. 9 stesso, anziché ridurne l'ambito di applicazione.

Questa impostazione, peraltro, risulterebbe ulteriormente problematica in quanto rischierebbe di escludere numerose attività di trattamento che comportano in concreto un elevato rischio per i diritti e le libertà degli interessati dal concetto di rischio rilevante per l'esecuzione di una valutazione d'impatto ai sensi dell'art. 35 del GDPR o per la nomina di un Data Protection Officer.

Modifiche in materia di diritto di accesso (Art. 12)

Il testo proposto dalla commissione prevede modifiche all'art. 12 che consentirebbero ai titolari di negare l'accesso ai dati personali qualora egli ritenga che la richiesta persegua scopi diversi dalla protezione dati o quando l'azienda "creda ragionevolmente" che la richiesta sia eccessiva.

Tale disposizione appare particolarmente preoccupante. In primo luogo, come considerazione sistemica, a fronte di semplificazioni e supporto nella circolazione dei dati, il nucleo centrale del GDPR e dei diritti da esso garantiti dovrebbe essere rafforzato, anziché diminuito. Diffatti, a catene di approvvigionamento dei dati più lunghe e maggiori scambi di informazioni, si dovrebbe rispondere garantendo agli interessi maggiori controlli e trasparenza.

Inoltre, viene trascurata l'utilità sociale che il diritto di accesso ai dati personali riveste. Anche quanto non strettamente correlato al tema del trattamento dei dati personali, esso viene sfruttato da giornalisti che verificano profilazioni, dipendenti che documentano trattamenti discriminatori, consumatori che contestano decisioni automatizzate; tali soggetti - alla luce della nuova formulazione - vedrebbero negato un diritto fondamentale sancito dall'Art. 8(2) della Carta UE, sulla base di una valutazione unilaterale del soggetto controllato.

Anche quando l'interpretazione della norma si spostasse nel senso di garantire comunque un accesso a tali fini, essi troverebbero da parte delle aziende titolari una maggiore opposizione e si vedrebbero costretti ad affrontare maggiori spese legali per il soddisfacimento dei propri legittimi diritti costituzionalmente garantiti.

Trasparenza nel trattamento dei dati (art 13)

La proposta prevede altresì una revisione dell'art. 13 del GDPR, nella misura in cui modifica il paragrafo 4 al fine di introdurre una più ampia e completa deroga all'obbligo di fornire l'informativa sul trattamento dei dati personali.

Questa nuova disposizione potrebbe risultare ampiamente lesiva dei diritti degli interessati in quanto aumenterebbe il novero delle situazioni in cui agli interessati non è fornita alcuna informazione sul trattamento dei propri dati personali.

Decisioni automatizzate (art. 22)

Inoltre, si segnala la modifica proposta all'art. 22 del GDPR che introduce un cambiamento significativo nel regime delle decisioni automatizzate. Secondo la nuova formulazione, una decisione che produce effetti giuridici o incide significativamente su un interessato può basarsi esclusivamente su un trattamento automatizzato, compresa la profilazione, se soddisfa determinati requisiti, tra cui il consenso esplicito, la previsione normativa e la necessità di concludere o eseguire un contratto tra l'interessato e un titolare del trattamento. In particolare, la modifica stabilisce che tale necessità sussiste "*indipendentemente dal fatto che la decisione possa essere presa con mezzi diversi da quelli esclusivamente automatizzati*".
Attualmente, invece, l'articolo 2 prevede che il titolare del trattamento debba dimostrare che la decisione automatizzata sia effettivamente **necessaria**, valutando anche la possibilità di adottare metodi più rispettosi della privacy. Se esistono alternative meno invasive, l'uso della decisione automatizzata per l'esecuzione di un contratto non sarebbe giustificato[3].

3 Cfr. Linee guida del Gruppo Articolo 29.

La modifica proposta, tuttavia, sembra attribuire al titolare del trattamento piena discrezionalità nell'utilizzo delle decisioni automatizzare, senza considerare se la decisione possa essere presa con metodi alternativi meno invasivi. Questo rappresenta un cambiamento di paradigma significativo, che potrebbe aumentare l'uso delle decisioni automatizzate e ridurre il coinvolgimento umano preventivo nella gestione dei contratti, con possibili ripercussioni sui diritti degli interessati.

Notifica violazioni (Art. 33)

Il testo prevede altresì una riformulazione dell'art. 33, secondo la quale la soglia di notifica obbligatoria dei data breach alle autorità di controllo passerebbe da "rischio" a "alto rischio".

In tal modo, le autorità di controllo perdono visibilità su incidenti medio-gravi, compromettendo sia la capacità di enforcement preventivo sia l'analisi statistica necessaria per identificare pattern sistemici delle violazioni.

Inoltre, il meccanismo di valutazione del rischio potrebbe piegarsi maggiormente ad utilizzi strumentali da parte delle aziende che, sfruttando la difficoltà di distinguere tra le differenti classi di rischio, potrebbero esentarsi dal notificare alle autorità di controllo violazioni gravi, indicative di violazioni dei diritti fondamentali o pratiche scorrette.

Accesso ai dispositivi terminali (Art. 88a)

L'Art. 88a introduce quattro nuove basi legali per l'accesso a dati "su o da" dispositivi terminali: trasmissione comunicazioni, servizio richiesto, informazioni aggregate, sicurezza.

Si riscontra, in tali casi, l'assenza di definizioni operative e l'effetto temuto è che la protezione dell'integrità del dispositivo (Art. 7 Carta UE) venga subordinata al regime GDPR[4].

---

4 Tra le pratiche in uso si vedano:: Microsoft Copilot Recall (screenshot continui del desktop), estrazione dati Android per training LLM, software kernel-level giustificato da "necessità di sicurezza".

Intelligenza Artificiale e interesse legittimo (Art. 88c)

Il nuovo Art. 88c qualifica automaticamente lo sviluppo e l'operazione di sistemi AI come interesse legittimo, eliminando il test di bilanciamento caso per caso. Difatti, il termine "operazione" copre qualsiasi utilizzo post-training, non solo l'addestramento iniziale.

In tal modo, il diritto di opposizione rimane formalmente preservato ma diventa materialmente irrealizzabile: opporsi a migliaia di titolari che processano gli stessi dataset richiede azioni individuali ripetute senza coordinamento possibile.

Corollario: Possibili Conseguenze Negative per l'Interazione tra EU GDPR ed AI Act

Collasso dell'enforcement (Articolo 6(3)) e assenza di trasparenza per gli interessati

Il Digital Omnibus modifica parallelamente il Regolamento AI. L'eliminazione dell'obbligo di registrazione per le esenzioni dall'Art. 6(3) AI Act consente ai fornitori di auto-esentarsi dalla classificazione high-risk senza comunicarlo pubblicamente.

Combinato con le modifiche GDPR un provider di sistemi di AI potrebbe, a seguito dell'esenzione e procedere al trattamento di dati per l'addestramento di sistemi di AI sulla base del legittimo interesse (Art. 88 c GDPR), eventualmente anche direttamente tramite il dispositivo sulla base del pretesto "servizio necessario" (Art. 88 a GDPR). In caso di violazione, peraltro, nessuna notifica sarebbe dovuta ai sensi del nuovo art. 33 del GDPR.

In questo modo, tuttavia, il diritto di opposizione diventerebbe inutile in quanto non vi è modo in cui l'interessato possa opporsi a trattamenti di dati personali effettuati tramite sistemi di cui non si conosce l'esistenza, operati da titolari che non devono dimostrare necessità, usando dati che dichiarano non personali. Tali titolari, inoltre, troverebbero nel nuovo art. 12 la base per negare ingiustificatamente, la richiesta di accesso ai dati personali.

Debiasing AI e categorie speciali (nuovo Art. 4a AI Act)

Il Digital Omnibus propone un nuovo Art. 4a che estende a tutti i sistemi AI (non solo high-risk) e ai deployer (non solo provider) la possibilità di processare categorie speciali di dati personali per correzione di bias, operazionalizzazione l'eccezione GDPR Art. 9(2)(g) "interesse pubblico sostanziale". Obiettivo dichiarato: colmare il gap per sistemi non high-risk che necessitano valutazione di equità. Le salvaguardie previste (pseudonimizzazione, controlli accesso, cancellazione post-correzione) rimangono identiche all'attuale Art. 10(5).

Il problema emerge nell'interazione con l'Art. 9 GDPR modificato. Un sistema può processare dati sensibili per debiasing sotto Art. 4a AI Act, ma sostenere che gli output inferenziali prodotti non costituiscano "categorie speciali" perché non "rivelano direttamente" informazioni sensibili (Art. 9 GDPR ristretto). Risultato: le salvaguardie Art. 4a si applicano al processing iniziale, ma i dati derivati—profilazioni su orientamento sessuale, affiliazione politica, condizioni di salute ottenute per inferenza—escono dal regime di protezione rafforzata. Il sistema formalmente rispetta i vincoli per il debiasing, ma utilizza poi liberamente le categorie sensibili inferite perché non coperte dall'Art. 9 modificato. Il conflitto definitorio tra i due articoli neutralizza la protezione operativa.

Eccezione biometrica e controllo del soggetto

L'Art. 9(2)(l) introduce un'eccezione per il trattamento di dati biometrici quando "sotto esclusivo controllo del soggetto interessato". Il concetto di "sole control" rimane indefinito operativamente.

Ad esempio, il Face ID su device Apple immagazzina template biometrici localmente, ma l'enclave sicura è gestita dal produttore. In tali casi, dove risiederebbe il controllo? I sistemi di autenticazione su device aziendali forniti al dipendente presentano ambiguità simili.

In tal senso, l'interazione con l'Art. 88a aggrava il problema: un sistema che accede a dati biometrici da terminal equipment per "servizio richiesto" può invocare simultaneamente l'eccezione "sole control", bypassando le restrizioni Art. 9 senza ricorrere alle eccezioni tradizionali che richiedono giustificazioni più stringenti.

Retention di categorie speciali in sistemi AI

L'Art. 9(5) richiede la rimozione di categorie speciali identificate nei dataset AI, ma introduce la clausola "disproportionate effort" come alternativa.
Poiché per i modelli linguistici già addestrati su miliardi di token, la rimozione post-training di dati sensibili è tecnicamente impossibile senza re-training completo, u controller possono sostenere che lo sforzo è sproporzionato, limitandosi a "proteggere i dati dall'essere usati per produrre output".
Difatti, il concetto di protezione post-hoc in modelli generativi già addestrati è tecnicamente nebuloso: il dato sensibile è già incorporato nei pesi del modello, il filtering applicato agli output non elimina l'informazione sottostante. La norma legalizza de facto la retention permanente di categorie speciali in AI systems quando la rimozione è costosa, usando uno standard non verificabile tecnicamente.

Assenza di coordinamento tra interesse legittimo AI e classificazione rischio

L'Art. 88c copre "sviluppo e operazione" di qualsiasi AI system senza distinguere tra tier di rischio dell'AI Act. Il riferimento alla definizione generica Art. 3(1) AI Act include sistemi prohibited, high-risk, limited risk e minimal risk indistintamente. Un sistema high-risk può invocare l'interesse legittimo presunto Art. 88c per processare dati personali "per operazione AI" senza che la norma richieda compliance preventiva ai requisiti di governance Art. 9-15 AI Act. GDPR e AI Act operano in parallelo senza meccanismi di interlock: l'Art. 88c fornisce base legale per processing indipendentemente dallo stato di conformità del sistema rispetto agli obblighi specifici della sua categoria di rischio. Il bilanciamento richiesto ("except where interests are overridden") avviene ex post, dopo che il processing è già iniziato sotto presunzione di legittimità.

Permanenza temporale dell'interesse legittimo AI

L'Art. 88c non prevede limiti temporali. Ogni altra base legale GDPR è contestuale: consenso revocabile, contratto legato a durata specifica, obbligo legale definito, interesse vitale emergenziale, public task circoscritto. L'interesse legittimo tradizionale richiede test di bilanciamento caso per caso. L'Art. 88c crea invece un interesse legittimo permanente e presunto per "operation of AI". La fase di development ha termine definito, ma "operation" è indefinita—finché il sistema è attivo, l'interesse sussiste.

Non è prevista review periodica della necessità, non c'è obbligo di dimostrare che il processing rimane necessario per specifici AI operation oltre il training iniziale. La retention dei dati può durare anni giustificata genericamente dall'operatività del sistema, senza re-assessment della proporzionalità o della minimizzazione rispetto all'evoluzione del sistema o delle sue finalità effettive.

Interazione test soggettivo e AI operation

La combinazione Art. 4(1) soggettivizzato e Art. 88c crea un percorso di data laundering strutturale. Un controller raccoglie dataset pseudonimizzato, dichiara di non possedere mezzi ragionevoli per re-identificare gli individui (quindi "non dato personale" ex Art. 4(1)), processa per training AI invocando Art. 88c come base legale residuale, e l'AI produce profili individuali accurati. Il controller sostiene che gli output non costituiscono dati personali "per sé" perché privo di mezzi per collegare profili a identità reali, anche quando downstream recipients—acquirenti dei profili—possiedono tali mezzi facilmente. L'Art. 4(1) modificato esplicita che l'informazione "*does not become personal for that entity merely because a subsequent recipient has means*".

Nessuna norma richiede al controller di considerare i *reasonable means* dei destinatari quando valuta se i dati sono personali durante il proprio processing. Il controller può intenzionalmente segregarsi dai mezzi di identificazione, processare massivamente per AI, distribuire output—operando fuori dal perimetro GDPR per l'intera catena perché "dati non personali per me". Il regime di accountability collassa quando la qualificazione di dato personale diventa scelta architettonica del titolare anziché proprietà oggettiva dell'informazione.