LE NUOVE LINEE GUIDA EDPB SULLA PSEUDONIMIZZAZIONE: UNA SVOLTA PER LA *PRIVACY BY DESIGN*

26 febbraio 2025

AUTORI

Aurora Agostini
Partner

Giulietta Minucci
Counsel

Giovanni Lombardi
Associate

Alessandro Carlini
Associate

Con le Linee Guida 01/2025, l'European Data Protection Board ("**EDPB**") ha fornito un'analisi approfondita sulla pseudonimizzazione, chiarendo i vantaggi, i requisiti normativi e le modalità di implementazione di questa misura tecnica e organizzativa prevista dal Regolamento Generale sulla Protezione dei Dati ("**GDPR**"). L'aspetto più rilevante del documento è l'approccio pragmatico adottato dall'EDPB, che riconosce la pseudonimizzazione non come un obbligo generalizzato, bensì come una misura che, se correttamente implementata, può risultare determinante per soddisfare molteplici requisiti normativi, dalla minimizzazione dei dati alla sicurezza del trattamento.

LA DEFINIZIONE DI PSEUDONIMIZZAZIONE E IL CONTESTO NORMATIVO

L'articolo 4(5) del GDPR definisce la pseudonimizzazione come "*il trattamento di 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*".

Con l'adozione delle Linee Guida, l'EDPB ha fornito un'interpretazione approfondita di questa definizione, elaborando per la prima volta un quadro completo sull'utilizzo di questa tecnica di protezione dei dati: il documento si inserisce in un contesto normativo in cui la pseudonimizzazione, pur non essendo un obbligo generalizzato, viene menzionata ripetutamente nel GDPR come una misura appropriata per adempiere a diversi obblighi di protezione dei dati.

In particolare, la pseudonimizzazione viene citata nel Considerando 28 come tecnica per ridurre i rischi per gli interessati, nel Considerando 29 come misura di sicurezza, nell'articolo 6(4)(e) come garanzia adeguata nel contesto dell'analisi di compatibilità dei trattamenti ulteriori, nell'articolo 25 come misura tecnica e organizzativa per la privacy by design e by default, nell'articolo 32 come misura di sicurezza, e nell'articolo 89 come garanzia appropriata per i trattamenti a fini di archiviazione, ricerca scientifica o storica e statistica.

Le Linee Guida EDPB chiariscono che questo istituto richiede l'attuazione di tre azioni fondamentali: (i) la modifica o trasformazione dei dati personali; (ii) la separazione delle informazioni aggiuntive necessarie per l'identificazione; (iii) l'applicazione di misure tecniche e organizzative per garantire la non attribuzione dei dati agli interessati. Un aspetto cruciale sottolineato dall'EDPB è che i dati pseudonimizzati rimangono dati personali, anche quando le informazioni aggiuntive sono conservate separatamente.

LA VALENZA DEL "*PSEUDONYMISATION DOMAIN*"

Particolarmente significativa è l'introduzione del concetto di "*Pseudonymisation Domain*", definito come il contesto in cui la pseudonimizzazione deve precludere l'attribuzione dei dati a soggetti specifici. Tale elemento rappresenta un'evoluzione concettuale che conferisce al Titolare del trattamento un'ampia discrezionalità nella delimitazione dell'ambito applicativo della pseudonimizzazione, potendo questo comprendere una singola unità organizzativa, un destinatario esterno specifico o tutti i destinatari legittimi previsti.

Pseudonimizzazione = dati non attribuibili senza informazioni aggiuntive

Questa flessibilità consente un'implementazione modulata in base all'effettiva valutazione del rischio, superando l'approccio "*one-size-fits-all*" che talvolta ha caratterizzato l'interpretazione di altre misure di sicurezza previste dal GDPR.

LA PSEUDONIMIZZAZIONE COME MISURA INTEGRATIVA NEL CONTESTO DI PROTEZIONE DEI DATI

Le Linee Guida sottolineano con chiarezza che la pseudonimizzazione, pur costituendo uno strumento prezioso all'interno dell'arsenale del Titolare per la compliance al GDPR, non deve essere considerata una soluzione isolata o autosufficiente. L'EDPB evidenzia, infatti, che tale tecnica raggiunge la sua massima efficacia quando implementata all'interno di un ecosistema di misure complementari, secondo un approccio integrato alla protezione dei dati.

Risulta particolarmente rilevante il principio espresso dall'EDPB secondo cui i Titolari del trattamento devono valutare l'adeguatezza di tutte le misure tecniche e organizzative nel loro complesso. Tale valutazione non può prescindere da una verifica concreta dell'efficacia della pseudonimizzazione nel prevenire l'attribuzione non autorizzata dei dati agli interessati, analisi che deve necessariamente tenere conto del contesto specifico del trattamento, delle tecnologie disponibili e delle risorse a disposizione di potenziali soggetti non autorizzati che potrebbero tentare di re-identificare gli interessati.

Il documento offre un'analisi dettagliata del ruolo della pseudonimizzazione nell'implementazione di diversi principi e requisiti previsti dal GDPR:

- privacy by design e by default (art. 25 GDPR): la pseudonimizzazione viene identificata come una delle misure tecniche e organizzative che il Titolare deve adottare "sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso". In questo contesto, l'EDPB distingue tra pseudonimizzazione applicata al trattamento interno e pseudonimizzazione finalizzata alla trasmissione a destinatari esterni, fornendo indicazioni specifiche per ciascuno scenario;
- trattamento basato sul legittimo interesse (art. 6(1)(f) GDPR): le Linee Guida precisano che la riduzione del rischio ottenuta mediante la pseudonimizzazione può essere considerata un fattore rilevante nella valutazione del bilanciamento degli interessi. In particolare, nei casi di dati sensibili o che potrebbero comportare discriminazioni significative, la pseudonimizzazione può contribuire a spostare l'ago della bilancia verso la prevalenza del legittimo interesse del Titolare rispetto agli interessi dell'interessato.
- compatibilità di trattamenti ulteriori (art. 6(4) GDPR): l'EDPB conferma che la pseudonimizzazione rappresenta una "garanzia adeguata" da considerare nella valutazione di compatibilità di un trattamento ulteriore rispetto alle finalità originarie. Particolarmente interessante è l'analisi dei casi in cui la pseudonimizzazione può rendere compatibile un'analisi statistica o una ricerca scientifica con finalità iniziali di natura commerciale o amministrativa.
- trasferimenti verso Paesi terzi (art. 44 e ss. GDPR): viene dedicata un'attenzione specifica alla pseudonimizzazione come misura supplementare per i trasferimenti internazionali, riprendendo i criteri già delineati nelle Raccomandazioni 01/2020. In questo ambito, l'EDPB specifica condizioni stringenti affinché la pseudonimizzazione possa essere considerata efficace, tra cui la necessità che le autorità del paese terzo non possiedano né possano ottenere con mezzi ragionevoli le informazioni aggiuntive.

Un elemento di particolare rilevanza riguarda l'interazione tra pseudonimizzazione e sicurezza del trattamento ex art. 32 GDPR: le Linee Guida chiariscono che una pseudonimizzazione efficace può attenuare la gravità delle conseguenze di un'eventuale violazione dei dati, riducendo potenzialmente gli obblighi di notifica ai sensi degli artt. 33 e 34 GDPR. Tuttavia, l'EDPB precisa che tale valutazione deve basarsi su un'analisi approfondita dell'effettiva robustezza delle tecniche di pseudonimizzazione implementate.

CONSIGLI PRATICI PER L'IMPLEMENTAZIONE DELLA PSEUDONIMIZZAZIONE

Alla luce delle Linee Guida, risulta opportuno definire un approccio sistematico all'implementazione della pseudonimizzazione, che tenga conto sia degli aspetti tecnici che di quelli organizzativi: di seguito, si propongono alcune indicazioni operative che possono costituire un framework di riferimento per i Titolari del trattamento.

In primo luogo, risulta essenziale la **definizione di una strategia documentata di pseudonimizzazione**. L'EDPB sottolinea, infatti, la necessità di adottare un approccio strutturato, che deve necessariamente prendere avvio dalla predisposizione di un documento programmatico nel quale vengano identificati gli obiettivi specifici della pseudonimizzazione nel contesto del trattamento considerato. Tale documento dovrebbe altresì contenere una delimitazione precisa del "Pseudonymisation Domain", individuando con chiarezza le entità

(persone fisiche, unità organizzative, soggetti esterni) che non dovranno essere in grado di attribuire i dati pseudonimizzati agli interessati. Ulteriori elementi da includere sono la mappatura dei flussi informativi relativi sia ai dati pseudonimizzati che alle informazioni aggiuntive, le procedure di governance per l'autorizzazione, l'esecuzione e la documentazione delle operazioni di de-pseudonimizzazione quando legittime e necessarie, nonché i criteri per la revisione periodica della strategia.

Privacy by design e by default: misura chiave per garantire la protezione fin dall'inizio

Per quanto concerne le **tecniche di trasformazione**, le Linee Guida forniscono un'analisi dettagliata, distinguendo principalmente tra algoritmi crittografici e tabelle di ricerca. Con riferimento ai primi, l'EDPB raccomanda l'utilizzo di funzioni crittografiche *one-way* (come HMAC o MAC) rispetto agli algoritmi di cifratura reversibile, in quanto offrono maggiore resistenza ai tentativi di inversione anche in caso di compromissione dei parametri segreti. In tale contesto, è necessario che il Titolare selezioni algoritmi con un adeguato livello di robustezza crittografica, implementi procedure sicure per la generazione e la gestione delle chiavi crittografiche e predisponga meccanismi per il rinnovo periodico dei parametri crittografici. Qualora, invece, si opti per l'utilizzo di tabelle di ricerca, occorrerà segregare fisicamente e logicamente tali tabelle, implementare controlli di accesso granulari e multi-livello, predisporre sistemi di logging avanzato per ogni consultazione e valutare l'opportunità di frammentare le tabelle su sistemi distinti. Appare inoltre di fondamentale importanza documentare la valutazione comparativa che ha portato alla scelta di una tecnica rispetto all'altra, con specifico riferimento ai rischi del contesto di trattamento.

Un elemento di particolare rilevanza nelle Linee Guida è l'attenzione dedicata ai quasi-identificatori, ovvero quegli attributi che, pur non essendo identificatori diretti, potrebbero consentire, singolarmente o in combinazione, la re-

identificazione degli interessati. A tal riguardo, il Titolare è chiamato a condurre un'analisi sistematica degli attributi presenti nei *dataset* da pseudonimizzare, classificandoli in base al loro potenziale identificativo, ed eseguire una valutazione quantitativa del rischio di re-identificazione: sulla base di tale analisi, dovranno essere implementate tecniche di generalizzazione, soppressione o randomizzazione, documentando il processo decisionale che ha portato alla selezione delle tecniche di mitigazione adottate.

Le Linee Guida evidenziano altresì un aspetto sovente trascurato nell'implementazione della pseudonimizzazione: la necessità di garantire **trasparenza agli interessati** e di predisporre procedure per l'esercizio dei loro diritti. In tale ottica, si rende opportuno integrare le informative privacy con specifiche sezioni dedicate alle pratiche di pseudonimizzazione, indicando le finalità per cui viene impiegata, le categorie di dati sottoposti a tale trattamento e i soggetti che hanno accesso ai dati pseudonimizzati e/o alle informazioni aggiuntive. Parimenti, dovranno essere predisposte procedure documentate per l'esercizio dei diritti, con particolare attenzione ai casi in cui l'interessato è in grado di fornire autonomamente lo pseudonimo associato ai propri dati, necessita di assistenza per individuarlo, ovvero risulta applicabile l'art. 11 GDPR, con conseguente limitazione di determinati diritti.

La robustezza delle misure di pseudonimizzazione deve, inoltre, essere oggetto di **verifica periodica**. In particolare, risulta consigliabile implementare un programma di test periodici sulle tecniche adottate, che comprenda test di penetrazione specificamente mirati a valutare la resistenza alla re-identificazione, simulazioni di attacchi basati su informazioni pubblicamente disponibili e valutazione dell'efficacia in scenari di data breach; tutti i risultati dovranno essere oggetto di un sistema di *reporting*.

Da ultimo, le Linee Guida sottolineano che **l'inversione non autorizzata della pseudonimizzazione costituisce una violazione dei dati personali** che può richiedere notifica all'autorità di controllo e comunicazione agli interessati. Si rende pertanto necessario aggiornare le procedure di gestione dei data breach, includendo criteri specifici per la valutazione della gravità delle violazioni che coinvolgono dati pseudonimizzati, procedure accelerate di risposta in caso di compromissione dei segreti di pseudonimizzazione e template documentali specifici per la notifica di violazioni relative a dati pseudonimizzati. È altresì consigliabile prevedere esercitazioni periodiche che simulino scenari di violazione coinvolgenti dati pseudonimizzati, con particolare attenzione all'inversione non autorizzata della pseudonimizzazione, alla compromissione delle informazioni

aggiuntive e ai linkage attack basati su dati provenienti da fonti diverse.

L'integrazione di questi elementi nel sistema di gestione della protezione dei dati consentirà al Titolare di massimizzare l'efficacia della pseudonimizzazione come

misura di sicurezza, garantendo al contempo la piena conformità con le indicazioni fornite dall'EDPB.

CONCLUSIONI

Le Linee Guida EDPB 1/2025 rappresentano un contributo determinante all'evoluzione interpretativa dell'istituto della pseudonimizzazione, colmando un vuoto esegetico che, sin dall'entrata in vigore del GDPR, aveva lasciato i Titolari privi di riferimenti sicuri; il documento, infatti, offre un sostegno concreto agli operatori, i quali dispongono finalmente di indicazioni operative per dare attuazione a questa importante misura di sicurezza, potendo così orientarsi nella complessità normativa che caratterizza il settore.

Va senz'altro apprezzato l'approccio pragmatico dell'EDPB che, abbandonando una visione astratta e monolitica della pseudonimizzazione, abbraccia una prospettiva contestualizzata e flessibile, fondata sull'analisi del rischio; tale impostazione, peraltro, permette ai Titolari di calibrare gli interventi in base alle peculiarità del trattamento, evitando così l'adozione di soluzioni preconfezionate che, oltre a risultare talvolta inefficaci, potrebbero rivelarsi sproporzionate rispetto alle finalità perseguite.

L'introduzione del concetto di "Pseudonymisation Domain" costituisce, in quest'ottica, un'innovazione di notevole pregio che, valorizzando il ruolo del Titolare nella perimetrazione dell'ambito applicativo della pseudonimizzazione, si inserisce coerentemente nel solco del principio di accountability; questa impostazione, infatti, riconosce al Titolare un margine di discrezionalità nell'individuazione dei soggetti che devono essere impossibilitati ad attribuire i dati pseudonimizzati agli interessati, mantenendo al contempo la responsabilità delle scelte operate.

Alla luce di quanto sopra, risulta quindi opportuno che i Titolari procedano a un riesame critico delle prassi di pseudonimizzazione già implementate, verificandone la rispondenza alle indicazioni dell'EDPB e, qualora necessario, adottando le misure correttive del caso; in particolare, assume rilievo centrale la documentazione delle valutazioni effettuate in merito alla perimetrazione del "Pseudonymisation Domain", alle tecniche di trasformazione prescelte e alle misure adottate per la gestione delle informazioni aggiuntive, in quanto tale documentazione costituisce il fulcro dell'*accountability* del Titolare.

Non va inoltre sottovalutata la valorizzazione della pseudonimizzazione quale strumento trasversale, idoneo a soddisfare molteplici requisiti normativi, sia nell'ambito della protezione dei dati by design e by default, sia quale misura per garantire un adeguato livello di sicurezza; ciò riveste particolare interesse nell'ambito dei trasferimenti di dati verso paesi terzi, ove la pseudonimizzazione può costituire, alle condizioni puntualmente indicate dall'EDPB, una misura

supplementare adeguata a garantire un livello di protezione sostanzialmente equivalente a quello assicurato nell'Unione Europea, contribuendo così a superare le criticità emerse a seguito della sentenza Schrems II.

In definitiva, le Linee Guida EDPB 1/2025 offrono una preziosa occasione per ripensare e rafforzare le strategie di protezione dei dati, inquadrando la pseudonimizzazione nel più ampio contesto delle misure di sicurezza e valorizzandone l'apporto alla realizzazione di un sistema complessivo di tutela dei dati personali; pertanto, gli operatori del settore sono chiamati a confrontarsi con questo importante documento, al fine di verificare la conformità delle proprie prassi e, ove necessario, adeguarle alle indicazioni dell'EDPB, così da garantire un'effettiva attuazione dei principi di *privacy by design* e *by default*, nonché un adeguato livello di sicurezza nel trattamento dei dati personali.

AUTORI

Aurora Agostini

Partner

Giulietta Minucci

Counsel

Giovanni Lombardi

Associate

Alessandro Carlini

Associate