LA FABBRICA DEGLI INGEGNERI
www.lafabbricadegliingegneri.it

**Dott. Ing. Claudio Valeri**
*Ingegnere Edile (VO) - Ingegnere Energetico e Nucleare (LM30)*
*Ordine degli Ingegneri della Provincia di Roma n°A23067*
*Prevenzione Incendi matricola del Ministero dell'Interno RM23067I03534*
*Consulente Tecnico del Tribunale di Velletri n°1443 Civile - n°157 Penale*
*Responsabile Servizio Prevenzione e Protezione (RSPP) modulo C – CSP – CSE (81/08)*
General Data Protection Regulation (GDPR) Regolamento UE 679/2016
*Professore di Costruzioni Progettazione Impianti, Tecnologia, Gestione del Cantiere e Sicurezza sui Luoghi di lavoro*
*Membro Commissione "Ingegneri Dipendenti" presso l'Ordine degli Ingegneri della provincia di Roma*
*Certificato Operatore di III° Livello come "Tecnico addetto alle prove non distruttive (PND)*
*nel campo dell'Ingegneria Civile e sui beni Culturali e Architettonici" nei seguenti metodi:*
*1) Ultrasonoro: PnD-CIV-0457 del 23/04/2018; 2) Sclerometrico: PnD-CIV-0458 del 23/04/2018;*
*3) Magnetometrico: PnD-CIV-0459 del 23/04/2018; 4) Monit. Strut. dei Quadri Fessurativi: PnD-CIV-0460 del 23/04/2018;*
*Certificato Operatore di II° Livello come "Tecnico addetto alle prove non distruttive (PND)*
*1) Ispezione e Monitoraggio di Ponti, Viadotti, Cavalcavia e Passerelle - PnD-CIV-0630 del 27/08/2018*

# GDPR e pseudonimizzazione: tecniche e regole di sicurezza per il corretto trattamento dati

La pseudonimizzazione è uno dei meccanismi di sicurezza previsto dal GDPR per aiutare titolari e responsabili del trattamento a proteggere i dati personali. Ecco, anche alla luce del documento specifico pubblicato da ENISA, le best practice per mettere in pratica questa importante misura tecnica.

## GDPR e pseudonimizzazione: come proteggere i dati personali

la **pseudonimizzazione è uno dei meccanismi di sicurezza** che il Reg. UE 2016/679 (GDPR) ha messo nero su bianco per aiutare i titolari e i responsabili del trattamento a **proteggere i dati personali**. All'articolo 4, la definisce come *"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"*.

In realtà, di pseudonimizzazione già parlava il Working Party 29 nella "*Opinion on Anonymisation Techniques*" (adottata il 10 aprile 2014) definendola come "la tecnica di sostituzione, in un record, di un attributo (tipicamente un attributo univoco) con un altro" e precisando, tuttavia, che, con tale procedimento, **i dati personali non sono anonimizzati** poiché "la persona fisica può continuare ad essere identificata, sebbene indirettamente".

Oggi la pseudonimizzazione costituisce una misura che dovrebbe essere largamente utilizzata dai titolari e dai responsabili facendo, tuttavia, molta attenzione ai riflessi che può avere sul trattamento dei dati personali.

LA FABBRICA DEGLI INGEGNERI
www.lafabbricadegliingegneri.it

**Dott. Ing. Claudio Valeri**
*Ingegnere Edile (VO) - Ingegnere Energetico e Nucleare (LM30)*
*Ordine degli Ingegneri della Provincia di Roma n°A23067*
*Prevenzione Incendi matricola del Ministero dell'Interno RM23067I03534*
*Consulente Tecnico del Tribunale di Velletri n°1443 Civile - n°157 Penale*
*Responsabile Servizio Prevenzione e Protezione (RSPP) modulo C – CSP – CSE (81/08)*
General Data Protection Regulation (GDPR) Regolamento UE 679/2016
*Professore di Costruzioni Progettazione Impianti, Tecnologia, Gestione del Cantiere e Sicurezza sui Luoghi di lavoro*
*Membro Commissione "Ingegneri Dipendenti" presso l'Ordine degli Ingegneri della provincia di Roma*
*Certificato Operatore di III° Livello come "Tecnico addetto alle prove non distruttive (PND)*
*nel campo dell'Ingegneria Civile e sui beni Culturali e Architettonici" nei seguenti metodi:*
*1) Ultrasonoro: PnD-CIV-0457 del 23/04/2018; 2) Sclerometrico: PnD-CIV-0458 del 23/04/2018;*
*3) Magnetometrico: PnD-CIV-0459 del 23/04/2018; 4) Monit. Strut. dei Quadri Fessurativi: PnD-CIV-0460 del 23/04/2018;*
*Certificato Operatore di II° Livello come "Tecnico addetto alle prove non distruttive (PND)*
*1) Ispezione e Monitoraggio di Ponti, Viadotti, Cavalcavia e Passerelle - PnD-CIV-0630 del 27/08/2018*

Via Aldo Moro n°47 -00048– Nettuno (Rm) **Tel./Fax:** 069804189; **Cell.** 3477629351

Si tratta, infatti, di sostituire un dato *vero* (direttamente collegabile ad una persona fisica e che chiameremo DV) con un dato *falso* (che non può essere riportato ad una persona fisica e che chiameremo DF) applicando un meccanismo segreto (che chiameremo S).

Quindi, se il dataset di partenza è il seguente:

| NOME E COGNOME | ETA' |
|---|---|
| MARIO ROSSI | 35 |
| GIUSEPPE VERDI | 48 |
| ANTONIO BIANCO | 57 |

l'obiettivo della pseudonimizzazione potrebbe essere quello di sostituire i DV (Mario Rossi, Giovanni Bianchi, Ernesto Verdi) con i DF contenuti in questa seconda tabella:

| DF | ETA' |
|---|---|
| RM | 35 |
| VG | 48 |
| BA | 57 |

Il meccanismo segreto S non pare, in questo esempio, particolarmente difficile da scoprire: i DF sono ottenuti dai DV prendendo le iniziali di cognome e nome. Questo esempio, sebbene esplicativo, appare abbastanza banale e, certamente, da non utilizzare per un paio di motivi:

- i DF contengono informazioni (le lettere iniziali) presenti nei DV e questo non è mai una buona pratica perché, in qualche modo, facilita un eventuale attaccante;
- il meccanismo segreto S può generare facilmente quelle che, in termini tecnici, sono chiamate *collisioni* ovvero se dovesse essere inserito nel dataset un nuovo soggetto che si chiama Erminio Villa lo pseudonimo corrispondente sarebbe lo stesso di Ernesto Verdi; questo è un caso assolutamente da evitare perché creerebbe ambiguità, per i soggetti titolati a farlo, nel risalire al soggetto cui i dati si riferiscono.

LA FABBRICA DEGLI INGEGNERI
www.lafabbricadegliingegneri.it

**Dott. Ing. Claudio Valeri**
*Ingegnere Edile (VO) - Ingegnere Energetico e Nucleare (LM30)*
*Ordine degli Ingegneri della Provincia di Roma n°A23067*
*Prevenzione Incendi matricola del Ministero dell'Interno RM23067I03534*
*Consulente Tecnico del Tribunale di Velletri n°1443 Civile - n°157 Penale*
*Responsabile Servizio Prevenzione e Protezione (RSPP) modulo C – CSP – CSE (81/08)*
General Data Protection Regulation (GDPR) Regolamento UE 679/2016
*Professore di Costruzioni Progettazione Impianti, Tecnologia, Gestione del Cantiere e Sicurezza sui Luoghi di lavoro*
*Membro Commissione "Ingegneri Dipendenti" presso l'Ordine degli Ingegneri della provincia di Roma*
*Certificato Operatore di III° Livello come "Tecnico addetto alle prove non distruttive (PND) nel campo dell'Ingegneria Civile e sui beni Culturali e Architettonici" nei seguenti metodi:*
*1) Ultrasonoro: PnD-CIV-0457 del 23/04/2018; 2) Sclerometrico: PnD-CIV-0458 del 23/04/2018;*
*3) Magnetometrico: PnD-CIV-0459 del 23/04/2018; 4) Monit. Strut. dei Quadri Fessurativi: PnD-CIV-0460 del 23/04/2018;*
*Certificato Operatore di II° Livello come "Tecnico addetto alle prove non distruttive (PND)*
*1) Ispezione e Monitoraggio di Ponti, Viadotti, Cavalcavia e Passerelle - PnD-CIV-0630 del 27/08/2018*

Via Aldo Moro n°47 -00048– Nettuno (Rm) **Tel./Fax:** 069804189; **Cell.** 3477629351

Occorre, quindi, utilizzare la pseudonimizzazione in maniera più sofisticata.

## GDPR e pseudonimizzazione: il valido "aiuto" dell'ENISA

In questo senso può tornare utile, come dicevamo all'inizio, il documento dell'ENISA che, nella parte iniziale, presenta:

- i possibili scenari di pseudonimizzazione rispetto ai ruoli che titolare (controller), responsabile del trattamento (processor) o terze parti (tipicamente contitolari) possono assumere nell'applicare questa misura;
- le tipologie di *attaccanti* rispetto alla possibilità di riuscire a scoprire il segreto S che renderebbe collegabili i dati a specifiche persone fisiche cioè di risalire dai DF ai DV e, quindi, riferire a soggetti precisi il resto dei dati presenti nel dataset.

Queste sezioni sono propedeutiche a motivare una delle conclusioni a cui giunge l'ENISA: **la pseudonimizzazione deve seguire un'attenta valutazione del rischio**. Questo perché **la pseudonimizzazione *costa* sia in fase di progettazione sia in fase di implementazione**.

Infatti, la parte più interessante del documento è nella presentazione di policy e tecniche di pseudonimizzazione: le prime sono quelle che definiscono l'approccio complessivo alla pseudonimizzazione mentre le seconde consentono di trasformare il singolo dato *vero* nel singolo dato *falso*.

La definizione di policy e tecniche diventa, quindi, un passaggio fondamentale per l'applicazione della *data protection by design* e hanno un impatto notevole sulla complessità del sistema finale e, naturalmente, sui costi di implementazione e sulle performance di esercizio.

Inoltre, come sottolinea l'ENISA, nell'effettuare le valutazioni bisogna tener conto che la facilità di impiego (di policy e tecniche) si contrappone, spesso, all'efficacia protettiva dei dati personali: più una tecnica (o una policy) è facile da progettare e implementare meno i dati risultano protetti.

Partita Iva: 07323021001
Codice Fiscale: VLRCLD71R09H501B
PEC: c.valeri@pec.ording.roma.it
MAIL: valericlaudio.cv@gmail.com

LA FABBRICA DEGLI INGEGNERI
www.lafabbricadegliingegneri.it

**Dott. Ing. Claudio Valeri**
*Ingegnere Edile (VO) - Ingegnere Energetico e Nucleare (LM30)*
*Ordine degli Ingegneri della Provincia di Roma n°A23067*
*Prevenzione Incendi matricola del Ministero dell'Interno RM23067I03534*
*Consulente Tecnico del Tribunale di Velletri n°1443 Civile - n°157 Penale*
*Responsabile Servizio Prevenzione e Protezione (RSPP) modulo C – CSP – CSE (81/08)*
General Data Protection Regulation (GDPR) Regolamento UE 679/2016
*Professore di Costruzioni Progettazione Impianti, Tecnologia, Gestione del Cantiere e Sicurezza sui Luoghi di lavoro*
*Membro Commissione "Ingegneri Dipendenti" presso l'Ordine degli Ingegneri della provincia di Roma*
*Certificato Operatore di III° Livello come "Tecnico addetto alle prove non distruttive (PND) nel campo dell'Ingegneria Civile e sui beni Culturali e Architettonici" nei seguenti metodi:*
*1) Ultrasonoro: PnD-CIV-0457 del 23/04/2018; 2) Sclerometrico: PnD-CIV-0458 del 23/04/2018;*
*3) Magnetometrico: PnD-CIV-0459 del 23/04/2018; 4) Monit. Strut. dei Quadri Fessurativi: PnD-CIV-0460 del 23/04/2018;*
*Certificato Operatore di II° Livello come "Tecnico addetto alle prove non distruttive (PND)*
*1) Ispezione e Monitoraggio di Ponti, Viadotti, Cavalcavia e Passerelle - PnD-CIV-0630 del 27/08/2018*

Via Aldo Moro n°47 -00048– Nettuno (Rm) **Tel./Fax:** 069804189; **Cell.** 3477629351

## Le tecniche di pseudonimizzazione

Per facilitare le valutazioni che titolare o responsabile del trattamento devono effettuare per scegliere policy e tecniche più adatte, conviene partire da una breve panoramica su queste ultime, esposte in ordine crescente di complessità computazionale:

- **tecnica del contatore** che consiste nell'assegnare ad ogni valore di DV un valore di DF generato da un contatore numerico che viene progressivamente incrementato di una quantità a piacere (ma fissa);
- **tecnica dei numeri casuali** che associa ad ogni valore di DV un valore di DF generato casualmente;
- **tecnica dell'hashing** che usa uno specifico algoritmo capace di associare ad un valore di DV di lunghezza arbitraria un valore di DF di lunghezza fissa e con la caratteristica che per valori diversi di DV crea valori diversi di DF;
- **tecnica dell'hashing con chiave** che, in termini di creazione di DF a partire da DV, opera in maniera identica all'hashing *semplice* usando un algoritmo basato su una chiave segreta;
- **tecnica della cifratura a chiave simmetrica** che, in termini di creazione di DF a partire da DV, opera in maniera identica all'hashing con chiave con la differenza che l'algoritmo di creazione di DF a partire da DV è dotato di un *algoritmo inverso* che trova DV a partire da DF.

Per tutte le tecniche elencate, eccetto che per la cifratura (dotata di algoritmo di decifratura), è necessario che il soggetto che pseudonimizza mantenga una tabella di corrispondenza DV-DF con queste caratteristiche:

- deve essere separata dai dati veri;
- deve essere sufficientemente protetta per evitare violazioni di riservatezza e di integrità.

LA FABBRICA DEGLI INGEGNERI
www.lafabbricadegliingegneri.it

**Dott. Ing. Claudio Valeri**
*Ingegnere Edile (VO) - Ingegnere Energetico e Nucleare (LM30)*
*Ordine degli Ingegneri della Provincia di Roma n°A23067*
*Prevenzione Incendi matricola del Ministero dell'Interno RM23067I03534*
*Consulente Tecnico del Tribunale di Velletri n°1443 Civile - n°157 Penale*
*Responsabile Servizio Prevenzione e Protezione (RSPP) modulo C – CSP – CSE (81/08)*
General Data Protection Regulation (GDPR) Regolamento UE 679/2016
*Professore di Costruzioni Progettazione Impianti, Tecnologia, Gestione del Cantiere e Sicurezza sui Luoghi di lavoro*
*Membro Commissione "Ingegneri Dipendenti" presso l'Ordine degli Ingegneri della provincia di Roma*
*Certificato Operatore di III° Livello come "Tecnico addetto alle prove non distruttive (PND) nel campo dell'Ingegneria Civile e sui beni Culturali e Architettonici" nei seguenti metodi:*
*1) Ultrasonoro: PnD-CIV-0457 del 23/04/2018; 2) Sclerometrico: PnD-CIV-0458 del 23/04/2018;*
*3) Magnetometrico: PnD-CIV-0459 del 23/04/2018; 4) Monit. Strut. dei Quadri Fessurativi: PnD-CIV-0460 del 23/04/2018;*
*Certificato Operatore di II° Livello come "Tecnico addetto alle prove non distruttive (PND)*
*1) Ispezione e Monitoraggio di Ponti, Viadotti, Cavalcavia e Passerelle - PnD-CIV-0630 del 27/08/2018*

Via Aldo Moro n°47 -00048– Nettuno (Rm) **Tel./Fax:** 069804189; **Cell.** 3477629351

## Le policy di pseudonimizzazione

L'approccio da impiegare man mano che il titolare o il responsabile si trova di fronte a nuovi elementi identificativi di persone fisiche da trattare è definito policy di pseudonimizzazione. In particolare, occorre decidere a priori:

- come trattare dati identificativi già presenti nei dataset;
- come trattare dati identificativi non presenti nei dataset.

Il funzionamento delle policy più classiche è riepilogato nella seguente tabella:

| **Casistica rispetto ai dati identificativi** | ***Dati identificativi già presenti nei dataset*** | ***Dati identificativi non presenti nei dataset*** |
|---|---|---|
| **Denominazione policy** | | |
| ***Pseudonimizzazione deterministica*** | Si usa lo stesso pseudonimo creato in precedenza | Si crea un nuovo pseudonimo da utilizzare anche per prossime occasioni |
| ***Pseudonimizzazione semicasuale*** | Si crea un nuovo pseudonimo se il dataset interessato è diverso da quello in cui erano presenti precedentemente i dati identificativi | Si crea un nuovo pseudonimo da utilizzare nel dataset interessato |
| ***Pseudonimizzazione casuale*** | Si crea sempre un nuovo pseudonimo | |

LA FABBRICA DEGLI INGEGNERI
www.lafabbricadegliingegneri.it

**Dott. Ing. Claudio Valeri**
*Ingegnere Edile (VO) - Ingegnere Energetico e Nucleare (LM30)*
*Ordine degli Ingegneri della Provincia di Roma n°A23067*
*Prevenzione Incendi matricola del Ministero dell'Interno RM23067I03534*
*Consulente Tecnico del Tribunale di Velletri n°1443 Civile - n°157 Penale*
*Responsabile Servizio Prevenzione e Protezione (RSPP) modulo C – CSP – CSE (81/08)*
General Data Protection Regulation (GDPR) Regolamento UE 679/2016
*Professore di Costruzioni Progettazione Impianti, Tecnologia, Gestione del Cantiere e Sicurezza sui Luoghi di lavoro*
*Membro Commissione "Ingegneri Dipendenti" presso l'Ordine degli Ingegneri della provincia di Roma*
*Certificato Operatore di III° Livello come "Tecnico addetto alle prove non distruttive (PND) nel campo dell'Ingegneria Civile e sui beni Culturali e Architettonici" nei seguenti metodi:*
*1) Ultrasonoro: PnD-CIV-0457 del 23/04/2018; 2) Sclerometrico: PnD-CIV-0458 del 23/04/2018;*
*3) Magnetometrico: PnD-CIV-0459 del 23/04/2018; 4) Monit. Strut. dei Quadri Fessurativi: PnD-CIV-0460 del 23/04/2018;*
*Certificato Operatore di II° Livello come "Tecnico addetto alle prove non distruttive (PND)*
*1) Ispezione e Monitoraggio di Ponti, Viadotti, Cavalcavia e Passerelle - PnD-CIV-0630 del 27/08/2018*

Via Aldo Moro n°47 -00048– Nettuno (Rm) **Tel./Fax:** 069804189; **Cell.** 3477629351

Due annotazioni importanti riguardanti le policy:

- la parola "casuale" nelle denominazioni delle policy non ha nessun riferimento al "casuale" delle tecniche di pseudonimizzazione;
- una volta stabilita la policy, può essere applicata qualsiasi tecnica di pseudonimizzazione.

## Le valutazioni del soggetto pseudonimizzante

Ma quali sono gli elementi che il soggetto pseudonimizzante (titolare, responsabile o terzo) deve tenere in considerazione per scegliere policy e tecniche? Tra gli altri, gli elementi più importanti sono:

- **dimensione del dataset che contiene i dati identificativi**; per dataset di dimensioni contenute potrebbe essere utilizzata la policy di pseudonimizzazione casuale e la tecnica del counter che costituiscono un buon bilanciamento tra efficacia di protezione (la policy) e semplicità di implementazione (la tecnica);
- **dimensione del flusso di nuovi dati identificativi**; quando il flusso di nuovi dati identificativi è notevole conviene affidarsi alla pseudonimizzazione casuale ed alla tecnica dell'hashing per evitare che i controlli sulla precedente presenza dei dati incida sulle performance;
- **numero di dataset interessati**; quando il numero di dataset interessati è minimo può essere utile applicare la policy di pseudonimizzazione semi-casuale ed una tecnica tra quelle più robuste come, per esempio, l'hashing con chiave;
- **necessità e frequenza di reidentificazione**; quando è necessario risalire con una certa frequenza all'identità dell'interessato, conviene utilizzare la pseudonimizzazione deterministica, come policy, e la cifratura a chiave simmetrica, come tecnica; quest'ultima, infatti, consente un immediato recupero dei dati identificativi senza necessità di consultazione della tabella di corrispondenza DV-DF;

LA FABBRICA DEGLI INGEGNERI
www.lafabbricadegliingegneri.it

**Dott. Ing. Claudio Valeri**
*Ingegnere Edile (VO) - Ingegnere Energetico e Nucleare (LM30)*
*Ordine degli Ingegneri della Provincia di Roma n°A23067*
*Prevenzione Incendi matricola del Ministero dell'Interno RM23067I03534*
*Consulente Tecnico del Tribunale di Velletri n°1443 Civile - n°157 Penale*
*Responsabile Servizio Prevenzione e Protezione (RSPP) modulo C – CSP – CSE (81/08)*
General Data Protection Regulation (GDPR) Regolamento UE 679/2016
*Professore di Costruzioni Progettazione Impianti, Tecnologia, Gestione del Cantiere e Sicurezza sui Luoghi di lavoro*
*Membro Commissione "Ingegneri Dipendenti" presso l'Ordine degli Ingegneri della provincia di Roma*
*Certificato Operatore di III° Livello come "Tecnico addetto alle prove non distruttive (PND) nel campo dell'Ingegneria Civile e sui beni Culturali e Architettonici" nei seguenti metodi:*
*1) Ultrasonoro: PnD-CIV-0457 del 23/04/2018; 2) Sclerometrico: PnD-CIV-0458 del 23/04/2018;*
*3) Magnetometrico: PnD-CIV-0459 del 23/04/2018; 4) Monit. Strut. dei Quadri Fessurativi: PnD-CIV-0460 del 23/04/2018;*
*Certificato Operatore di II° Livello come "Tecnico addetto alle prove non distruttive (PND)*
*1) Ispezione e Monitoraggio di Ponti, Viadotti, Cavalcavia e Passerelle - PnD-CIV-0630 del 27/08/2018*

Via Aldo Moro n°47 -00048– Nettuno (Rm) **Tel./Fax:** 069804189; **Cell.** 3477629351

- **disponibilità di risorse computazionali e di memorizzazione**; è chiaro che occorre fare i conti con le capacità computazionali e di memorizzazione disponibili visto che alcune policy (pseudonimizzazione deterministica) e alcune tecniche (hashing con chiave e cifratura a chiave simmetrica) possono essere piuttosto impegnative in termini di capacità di calcolo e/o spazio necessario;

oltre che, naturalmente, il **livello di rischio** associato al trattamento dei dati personali che dipende dal servizio fornito, dal contesto della fornitura e dalla tipologia di dati trattati.

## GDPR e pseudonimizzazione: l'importanza del segreto

Per molte tecniche di pseudonimizzazione è necessario che il soggetto pseudonimizzante mantenga una tabella di corrispondenza DV-DF per poter reidentificare l'interessato (per fornire il servizio piuttosto che per adempiere correttamente ad una richiesta di esercizio dei diritti previsti dal GDPR).

Questo implica che la tabella di corrispondenza è parte integrante (insieme alla modalità di calcolo dello pseudonimo) del segreto S e, quindi, per evitare violazioni di integrità e riservatezza, va tutelata memorizzandola in un posto diverso dai dati e sottoponendola ad una adeguata cifratura.

Tuttavia, è altresì importante che la tabella di corrispondenza sia sempre disponibile e che non si incorra nel paradosso della "eccessiva protezione", per esempio, affidando le chiavi di cifratura ad un solo soggetto che, magari, lascia l'organizzazione portandosele appresso ancorché del tutto in buona fede. In questo caso si incorrerebbe in una violazione di disponibilità e l'organizzazione pseudonimizzante (titolare, responsabile o terzo) non potrebbe far fronte, per esempio, a richieste di accesso ai sensi dell'art. 15 del GDPR.

Occorre, quindi, progettare (data protection by design) una gestione del segreto finalizzata a bilanciare correttamente riservatezza, integrità e disponibilità.