POLICY
PSEUDONIMIZZAZIONE E CIFRATURA DEI DATI

COD. C.08
VERS. 01 DEL 05.2022

CONTIENE:

1. **POLICY**

INDICE DELLE VERSIONI SUCCESSIVE ALLA PRIMA:

COD. VERSIONE	DATA MODIFICA	MODIFICHE

PREMESSA

Un *data breach* consiste in una violazione della sicurezza che comporta – accidentalmente o illegalmente – la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali, trasmessi, archiviati o altrimenti elaborati. Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità dei dati personali. La pseudonimizzazione e la cifratura dei dati personali sono due misure che se correttamente applicate possono, tra l'altro, ridurre i rischi di incorrere in *data breach.*

PSEUDONIMIZZAZIONE

Con il termine **pseudonimizzazione** viene indicato il processo di trasformazione attraverso il quale un dato personale non è più riferibile, in assenza di informazioni aggiuntive, ad un soggetto identificato, ossia all'interessato al quale appartengono i dati. Tipicamente, questa dissociazione avviene sostituendo uno o più identificatori personali (ad esempio: nome, cognome, e-mail ecc.) con identificatori pseudonimi (c.d. *alias*), che permettono la ricostruzione dell'identità dell'utente solo mediante l'impiego di aggiuntive informazioni (ad esempio: correlazione identificatore personale /identificatore pseudonimo).

Ne consegue che, a fronte di un dataset in input, il processo di pseudonimizzazione ne restituisce due in output, ossia il dataset pseudonimizzato, modificato rispetto al dato originale, e il data set di transcodifica. Per la ricostruzione del dato originale, quindi, è necessario accedere congiuntamente ad entrambi i dataset. Per la caratteristica di reversibilità del processo di pseudonimizzazione, le informazioni che consentono la reidentificazione dell'interessato, a partire dai dati pseudonimizzati, devono essere conservate separatamente e protette, a loro volta, con misure di sicurezza efficaci, come la segregazione della chiave di cifratura, l'adozione di soluzioni key manager e la separazione fisica degli ambienti di conservazione del dato pseudonimizzato e delle informazioni di riconversione.

BENEFICI DELLA PSEUDONIMIZZAZIONE

La pseudonimizzazione permette di:

- Nascondere l'identità dei soggetti, a cui i dati sono riferiti, a chiunque non ne sia autorizzato (terze parti), pur mantenendo la congruità semantica di ciascun dataset (dataset pseudonimizzato/dataset di transcodifica);
- Garantire il rispetto dei principi della minimizzazione del dato e del "need to know", laddove le informazioni relative all'identificazione del soggetto interessato non siano necessarie, ad esempio, alle finalità del trattamento. La separazione del dataset pseudonimizzato dalla tabella di transcodifica consente di soddisfare i requisiti normativi imposti dagli artt. 4, 5, 25 e 32 del GDPR, limitando l'accesso alle sole informazioni necessarie al trattamento.

ESEMPI DI PSEUDONIMIZZAZIONE:

Sebbene la pseudonimizzazione così come descritta dal GDPR e dalle *best practice* ENISA sia una misura tecnica ed organizzativa di non facile implementazione da parte delle scuole, è opportuno comunque focalizzare una serie non esaustiva di casistiche dove dovrebbe essere utilizzata al fine di ridurre il più possibile i rischi di *data breach* e al contempo contenere i rischi dei trasferimenti di dati extra UE connessi all'utilizzo della G-Suite:

1. **Pseudonimizzazione degli indirizzi mail degli alunni**: questa misura di protezione prevede che la scuola abbia implementato un regolamento informatico che indichi espressamente tra le altre il soggetto responsabile di mettere in atto questa misura, quale logica è stata utilizzata per creare gli pseudonimi, per quale tipologia di utenti viene utilizzata, chi si trova in possesso delle informazioni aggiuntive per accedere ai dati personali, le tempistiche di revisione della procedura.
2. **Pseudonimizzazione dei PDP/PEI in G-Suite**: strutturare i PDP e i PEI con i dati in chiaro in Google è molto rischioso per i diritti e le libertà degli interessati. Infatti, la G-Suite sebbene sia uno strumento molto potente, va utilizzato mettendo in atto tutte le misure tecniche ed organizzative del caso per poter operare nella legalità. Non è *privacy compliant* associare i PDP / PEI all'interessato Mario Rossi M.R. poiché l'alunno potrà risultare facilmente identificabile da Google, è invece *privacy compliant* adottare delle vere e proprie procedure di pseudonimizzazione descrittive della fase di strutturazione, comunicazione, conservazione e archiviazione dei dati e delle informazioni. Per la validazione di queste procedure è opportuno contattare anche il DPO.
3. **Pseudonimizzazione delle comunicazioni mail**: è opportuno che il personale scolastico si abitui a rendere le comunicazioni mail il meno identificabili possibili utilizzando quanto meno delle forme di pseudonimizzazione (i.e. anziché Mario Rossi riportare M.R.)

e meglio ancora dei veri e propri pseudonimi.

PROCESSO	TECNICA DI PSEUDONIMIZZAZIONE	MISURE DA ATTUARSI
INDIRIZZI MAIL	complessa	Costituzione di un regolamento informatico
PEI / PDP	complessa	Predisposizione di adeguata procedura
COMUNICAZIONE MAIL	Semplice	Indicazioni del Dirigente scolastico oltreché del DPO
INDICARE PROCESSO		

DIFFERENZA TRA PSEUDONIMIZZAZIONE BY DESIGN E CIFRATURA

La cifratura (encryption) è un processo di offuscamento del dato che, mediante l'impiego di un algoritmo matematico, restituisce un output non intellegibile da parte di un utente che non possiede la chiave di decifratura. La cifratura, quindi, è un particolare processo di pseudonimizzazione, che presenta le seguenti caratteristiche: (*i*) a partire da un dataset iniziale ne restituisce esclusivamente uno cifrato; (*ii*) le informazioni cifrate sono completamente non intellegibili da un soggetto terzo, viene meno la riconducibilità al dato originale e il valore semantico del dato stesso.

Come per la pseudonimizzazione la crittografia è una misura di protezione di non facile predisposizione. Ciò nonostante, la crittografia può trovare applicazione in forma semplice in alcuni trattamenti di dati messi in atto dal personale scolastico.

PROCESSO	TECNICA DI CRITTOGRAFIA	MISURE DA ATTUARSI
Memorizzazione dei dati su chiavetta USB	Crittografia simmetrica	Utilizzo di chiavette crittografate o inserimento password sulla singola cartella o sul singolo file
Comunicazione di elenchi di dati personali via mail	Crittografia simmetrica	Inserimento password sul singolo file con comunicazione della stessa attraverso mezzo diverso
INDICARE PROCESSO		

Si fa inoltre presente che in caso di perdita o furto di device i cui dati non siano stati crittografati sarà comunque necessario non solo documentare la perdita del device all'interno del registro delle violazioni ma anche comunicare il *data breach* all'Autorità Garante.

	REGISTRO DELLE VIOLAZIONI	COMUNICAZIONE ALL'AUTORITÀ GARANTE	COMUNICAZIONE AGLI INTERESSATI
DEVICE CON DATI NON CRITTOGRAFATI	SI	SI	Non esclusa qualora sulla chiavetta siano eventualmente (anche se non dovrebbero) conservati categorie particolari di dati personali
DEVICE CON DATI CRITTOGRAFATI	SI	NO	NO