

Prot. vedi segnature

Bisuschio, 15 .09.2023

Circolare n.22

**A tutto il personale Docente e ATA
Alle Famiglie
Atti/Sito/Albo**

Oggetto: Designazione del Responsabile della protezione dei dati e obbligo di gestione e notifica delle violazioni dati personali (cd. "data breach") alla luce delle linee guida EDPB 9/2022

VISTO il **Regolamento UE 2016/679** relativo alla protezione delle persone fisiche con riguardo al VISTE trattamento dei dati personali, nonché alla libera circolazione di tali dati (regolamento generale sulla protezione dei dati), detto anche brevemente GDPR, da General Data Protection Regulation.

VISTE le nuove **linee guida EDPB 09/2022** (European Data Protection Board) sulla gestione e la notifica delle violazioni di dati personali (c.d. "data breach") che chiariscono gli obblighi di notifica che sussistono, rispetto alle Autorità Garanti e agli interessati, nel caso in cui si verifichi una violazione dei dati personali, allo scopo di supportare i Titolari e Responsabili del trattamento nella gestione degli incidenti di sicurezza eventualmente occorsi all'interno delle proprie organizzazioni.

CONSIDERATO che le linee guida **EDPB 09/2022** hanno rilevanza anche per le istituzioni scolastiche

VISTA la **nota 1248** emessa dal **Ministero dell'Istruzione e del Merito** in data 28/7/2023 con oggetto "Obblighi di notifica in caso di violazione dei dati personali".

CONDIDERATO che in base al principio di accountability spetta al titolare del trattamento l'onere di adottare misure tecnico/organizzative atte a minimizzare la probabilità di violazione degli stessi dati.

TUTTO CIÒ PREMESSO ed in ottemperanza a tale onere, il **titolare del trattamento dati**, nella persona della **Dirigente scolastica prof.ssa Maria Carmela Sferlazza** dell'Istituto Valceresio, ha provveduto a designare il Responsabile della protezione dei dati nellapersona del **Ing. Vargiu Antonio per la società Vargiu scuola S.r.l.** Tutti gli interessati (dipendenti, genitori, alunni, fornitori etc.) possono contattare il DPO all'indirizzo dpo@vargiuscuola.it oppure al numero **070 284300**, per porre qualsiasi quesito relativo alla normativa in materia di sicurezza e protezione dei dati, o relativo all'esercizio dei numerosi nuovi diritti dell'interessato introdotti dal **GDPR** e dalle linee guida **EDPB 09/2022**

In osservanza a quanto previsto dall'art. 37 comma 7 del GDPR, i dati di contatto del DPO sono stati comunicati al Garante per la protezione dei dati personali e saranno resi pubblici sul sito web istituzionale dell'Ente.

Tutti i soggetti, sia pubblici che privati, hanno l'obbligo di notificare al Garante per la protezione dei dati personali,

entro 72 ore, alcune tipologie di evento riconducibili alla fattispecie di “**violazione dei dati personali**”.

È pertanto necessario che tutto il personale sappia precisamente che cosa è una violazione dei dati personali, e le varie forme attraverso le quali tale evento può accadere.

Il GDPR all’art. 4 punto 12, fornisce la seguente definizione di violazione dei dati personali:

“la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai dati personali trasmessi, conservati o comunque trattati”. Inoltre le **nuove linee guida 9/2022**, ribadiscono che le violazioni possono essere classificate in base ai seguenti tre principi ben noti della sicurezza delle informazioni:

- “violazione della riservatezza”, in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
- “violazione dell’integrità”, in caso di modifica non autorizzata o accidentale dei dati personali;
- “violazione della disponibilità”, in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

Contrariamente a quanto si potrebbe pensare, pertanto, la definizione di “*violazione di dati personali*” contempla non solo le fattispecie in cui vi sia stato un accesso abusivo ai dati personali, ma anche il caso della distruzione o della perdita dei dati personali, eventi che si possono verificare con una certa frequenza, ad esempio a causa del guasto di un supporto di memorizzazione, di un virus informatico, di un non corretto svolgimento delle procedure di *backup*, etc. Oppure può riguardare la casistica di dati personali o sensibili comunicati o portati a conoscenza di soggetti, interni o esterni all’Istituto, non autorizzati o non titolati.

Tra le casistiche di violazione dei dati personali che si possono verificare possiamo citare le seguenti:

- smarrimento di una chiavetta USB contenente dati personali
- furto di PC o tablet contenenti dati personali
- violazione del Registro elettronico
- smarrimento o furto di verifiche degli alunni
- non custodire adeguatamente i dati vaccinali
- portare a conoscenza dati di un alunno al genitore per il quale sia stato emesso un Provvedimento da parte del Tribunale dei minori di revoca della potestà genitoriale
- soddisfare una richiesta di accesso agli atti, che comporti la violazione della privacy del c.d.

“controinteressati”

- pubblicare dati personali eccedenti rispetto a quelli strettamente indispensabili per il raggiungimento delle finalità.

- Una e-mail che viene inviata ai destinatari nei campi “a:” o “cc:”, consentendo così a ciascun destinatario di vedere l’indirizzo e-mail di altri destinatari.
- Dati e documenti criptati da un ransomware (malware del riscatto).
- Dati e documenti criptati dal titolare del trattamento mediante una chiave non più in suo

possesso.

È importante inoltre ricordare che la violazione dei dati personali non riguarda solamente i dati in formato elettronico, ma può riguardare anche i dati in formato cartaceo; questa seconda casistica, anzi, è la più critica da gestire, in quanto se vi fosse la perdita o il furto di fascicoli cartacei contenenti dati personali, tale evenienza potrebbe essere molto difficile da rilevare.

Nel dettaglio, l'art. 33 del Regolamento UE 2016/679 prevede:

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

3. La notifica di cui al paragrafo 1 deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.”

Inoltre, l'art. 34 del Regolamento UE 2016/679 prevede:

“1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).

3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle

seguenti condizioni:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analogo efficacia.

4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.”

Si chiede, pertanto, di porre la massima attenzione nel monitorare e rilevare tempestivamente tutti gli eventi di tipo “*violazione dei dati personali*”, compresi gli eventi per i quali non vi sia la certezza ma anche solo un sospetto, e comunicarli immediatamente al Dirigente Scolastico, il quale provvederà ad informare tempestivamente il DPO, che provvederà ad effettuare tutte le valutazioni del caso di concerto con il Dirigente Scolastico ed a predisporre, se ve ne siano i presupposti, la notificazione da effettuare entro 72 ore all’Autorità di Controllo nazionale (Garante per la protezione dei dati personali). Si ricorda che la tardiva od omessa notificazione al Garante di un evento di tipo “*violazione dei dati personali*” è punita con la sanzione amministrativa pecuniaria fino a 10.000.000,00 di Euro, ai sensi dell’art. 83 comma 4 lettera a) del Regolamento Europeo.

Il Dirigente Scolastica

Maria Carmela Sferlazza

Firma digitale apposta ai sensi dell’art. 21
D.Lgs. 82/20(Codice dell’Amministrazione Digitale)