Protocollo 0009603/2026 del 29/07/2026 08:13:26

FUTURA LA SCUOLA PER L'ITALIA DI DOMANI
Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Istruzione e del Merito
Italiadomani
ISTITUTO STATALE ISTRUZIONE SUPERIORE
VALCERESIO
Liceo Scientifico - Scienze Applicate
Liceo delle Scienze Umane
Istituto Tecnico Turismo
Istituto Tecnico Amministrazione, Finanza e *Marketing* - Relazioni Internazionali
Istituto Professionale per la Sanità e l'Assistenza sociale
ISIS VALCERESIO BISUSCHIO
Via Roma, 57 - 21050 Bisuschio (VA) - ☎ Tel. 0332856760 - Fax 0332474918 - vais00400r@istruzione.it

Bisuschio, 28/07/2026

Ai Docenti
Al Personale ATA
ATTI/SITO

Oggetto: Informativa privacy – "Data Breach - Obbligo di notifica delle violazioni dei dati"
A.S. 2026/2027

Tra le numerose disposizioni introdotte dal GDPR, vi è l'obbligo per tutte le Pubbliche Amministrazioni di designare, ai sensi dell'art. 37, il **Responsabile della protezione dei dati**, detto anche **DPO**, da Data Protection Officer.
Come già comunicato, in ottemperanza a tale obbligo, per l'a.s. 2025/26 l'Istituto ha provveduto a designare il Responsabile della protezione dei dati nella persona dell'**Ing. Antonio Vargiu**, di Vargiu Scuola S.r.l.
Tutti gli interessati (dipendenti, genitori, alunni, fornitori etc.) possono contattare il DPO all'indirizzo commerciale@vargiuscuola.it oppure ai numeri 070271526 - 070271560, 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.
Una seconda significativa disposizione introdotta dal GDPR è l'obbligo per tutti i soggetti, sia pubblici che privati, di notificare al Garante per la protezione dei dati personali, alcune tipologie di evento riconducibili alla fattispecie di "**violazione dei dati personali**". Pertanto è necessario che tutto il personale venga formato ed informato in merito alla violazione dei dati personali e alle varie forme attraverso le quali tale evento può accadere.

Il **GDPR all'art. 4 paragrafo 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***". 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.

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 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 GDPR 2016/679 "Notifica di una violazione dei dati personali all'autorità di controllo" 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 GDPR 2016/679 "Comunicazione di una violazione dei dati personali all'interessato"** prevede:

1. *Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per*

2. *i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.*

3. *da 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).*

4. *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 analoga efficacia.

5. *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 ai sensi dell'**art. 83** del GD2016/679.

Linee Guida n. 09/2022 sulla gestione e la notifica delle violazioni di dati personali

Si coglie l'occasione per comunicare che verrà attivato il corso obbligatorio di formazione docenti e ATA sulla privacy organizzato dal DPO Vargiu, della durata media di 3h - seguirà apposita circolare.

.

La Dirigente Scolastica
Maria Carmela Sferlazza
Firma autografa sostituita a mezzo stampa, ai sensi dell'art. 3, comma 2 del D.Lg. 39/93