



## Ministero dell'Istruzione

### ISTITUTO COMPRENSIVO DI TIRANO

Via Pedrotti n. 17 – 23037 TIRANO (SO) - Tel. 0342/701138 – Fax 0342/711007  
E-mail ministeriale: [soic81800g@istruzione.it](mailto:soic81800g@istruzione.it) – e-mail PEC: [soic81800g@pec.istruzione.it](mailto:soic81800g@pec.istruzione.it)  
Codice Meccanografico: SOIC81800G - CODICE FISCALE: 92024630144

AL PERSONALE DOCENTE  
AL PERSONALE ATA  
AI COLLABORATORI ESTERNI  
AL SITO WEB - AGLI ATTI

#### **Oggetto: Comunicazione relativa alla gestione della violazione dei dati (cd. “Data Breach”)**

La presente circolare si prefigge lo scopo di indicare le opportune modalità di gestione della violazione dei dati personali, cd. “Data Breach”, nel rispetto della normativa in materia di trattamento dei dati personali e dei principi e delle disposizioni contenute dal Regolamento UE 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

La nozione di violazione dei dati personali è contenuta nell’art. 4, punto 12 del Regolamento UE n. 679/2016: *“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”*.

La definizione di “violazione di dati personali”, contenuta nell’art. 4, punto 12 del Regolamento UE n. 679/2016, 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. Verosimilmente, può riguardare dei dati personali o sensibili comunicati o portati a conoscenza di soggetti, interni o esterni all’Istituto, non autorizzati o non titolari.

La violazione dei dati personali non riguarda solamente i dati in formato elettronico, ma può riguardare anche i dati in formato cartaceo. Quest’ultima fattispecie è 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.

Una violazione dei dati personali, se non affrontata in modo adeguato e tempestivo, può provocare danni fisici, materiali ed immateriali alle persone coinvolte. Per tali ragioni, tale circolare ha intento di delineare le procedure specifiche di gestione di una violazione dei dati personali, sia che avvenga all’interno e sia all’esterno della struttura.

Ogni operatore autorizzato a trattare i dati personali, qualora venga a conoscenza di un potenziale caso di “data breach”, avvisa tempestivamente il Titolare del trattamento. Quest’ultimo, valuta l’evento, se confermate le preoccupazioni di una potenziale violazione dei dati personali, lo segnala tempestivamente al Data Protection Officer. Ai sensi dell’art. 33 del Regolamento UE n.

679/2016, il D.P.O. predispone l'eventuale comunicazione all'Autorità Garante, a firma del titolare, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, da determinarsi dal momento in cui il titolare ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza della verifica di un incidente di sicurezza che riguardi dati personali. Oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo.

E' comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il titolare venga a conoscenza, a seguito della effettuazione di ulteriori indagini.

Ai sensi dell'art. 34 del Regolamento UE n. 679/2016, nel caso in cui dal data breach possa derivare un rischio elevato per i diritti e le libertà delle persone, anche queste devono essere informate senza ingiustificato ritardo, al fine di consentire loro di prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione. Il Titolare del trattamento predispone l'eventuale comunicazione agli interessati da inviarsi nei tempi e nei modi che lo stesso,

L'art. 34 del Regolamento UE. N. 679/2016 continua affermando che: *“Non è richiesta la comunicazione all'interessato, 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;*
- 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.*

*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, sopra indicate, è soddisfatta.”*

Si chiede a tutto il personale e ai collaboratori esterni 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 Responsabile della protezione dei dati dell'Istituto designato ai sensi dell'art. 37 del GDPR, 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 UE n. 679/2016.

DIRIGENTE SCOLASTICO  
Elena Panizza