**LICEO STATALE "G. CARDUCCI"**
Via S.Zeno 3 - 56127 Pisa
***Scienze Umane, Linguistico, Economico-sociale, Musicale***

tel.: +39 050 555 122 - fax: +39 050 553 014 - email: pipm030002@istruzione.it - pec: pipm030002@pec.istruzione.it
sito: https://www.liceocarducci.edu.it - cod. mecc.: PIPM030002 - cod. fiscale: 80006190500 - cod. univoco ufficio: UFK69O

LICEO STATALE - "G. CARDUCCI"-PISA
Prot. 0011325 del 28/09/2023
III (Uscita)

**Pisa 28 settembre 2023**

**All'intero personale del Liceo**

**Circolare: 34**

**OGGETTO: OBBLIGO DI NOTIFICA DELLE VIOLAZIONI DEL DATI (CD. "DATA BREACH")**

Con la presente circolare si evidenzia che l'art. 33 del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libertà di circolazione di tali dati, del nuovo Regolamento generale sulla protezione dei dati, prevede l'obbligo da parte di tutte le Pubbliche Amministrazioni di **comunicare al Garante** per la protezione dei dati personali qualsiasi evento di "**violazione di dati personali**".

Lo stesso Regolamento UE 2016/679, 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".

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, casistica fortunatamente abbastanza rara, ma anche il caso della distruzione o della perdita dei dati personali, che invece sono 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.

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'art. 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 punto 1 deve almeno:

> a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessi 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 fomite in fasi successive senza ulteriore ingiustificato ritardo.

5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze ad 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 punto 1 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'art. 33, paragrafo 3, lettere b), c) e d).

3. Non è richiesta la comunicazione all'interessato di cui al punto 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 punto 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.

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 rischia elevato, che vi provveda o può decidere che una delle condizioni di cui al punto 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 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" ed è punita con gravose sanzioni ai sensi dell'art. 83 comma 4 lettera a) del Regolamento Europeo.

Si invitano tutti i dipendenti in servizio a consultare periodicamente le informazioni e i documenti pubblicati nella sezione "Privacy", rinvenibile all'Area Riservata del sito del Ministero e a prendere visione del Regolamento nella sezione privacy del sito web istituzionale "Regolamento data breach".

Cordiali saluti.

La Dirigente Scolastica
*Prof.ssa Sandra Capparelli*
Firmato digitalmente