LICEO STATALE "G. FRACASTORO"
Via G.B. Moschini,11/A; tel. 045 8348772; fax 045 8343626;
sitoweb: www.liceofracastoro.edu.it - Email vrps03000r@istruzione.it
V E R O N A

Circ. n.499 Verona'16 Maggio 2022

Ai Docenti
Al personale ATA
Al DSGA
Al DPO
All'Animatore Digitale
All' Amministratore di sistema
All'AT per l'informatica
Agli Atti

**Oggetto: Procedura gestione violazione dati personali (data breach)**

Il Regolamento Europeo 679/2016 (da ora GDPR) impone al titolare del trattamento di dati personali la definizione di misure tecniche ed organizzative finalizzate a garantire la protezione dei dati personali trattati dal Liceo. Il Dirigente scolastico – rappresentante legale dell'Istituzione scolastica e titolare del trattamento – ha predisposto la presente procedura per la gestione delle violazioni *privacy,* con particolare riferimento alle procedure adottate per la gestione dei *data breach.*
Alla luce del GDPR, si tratta delle misure organizzative ad oggi ritenute più idonee a tutelare i dati personali trattati.

**1 - DEFINIZIONE: COSA È UNA VIOLAZIONE DI DATI PERSONALI (*DATA BREACH*)**

L'articolo 4, punto 12, del GDPR definisce il *data breach* come «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».

È bene, anzitutto, precisare che, affinché possa parlarsi di *data breach*, è necessario che la **violazione riguardi dati riferibili ad una persona o a più persone**. Risulta, pertanto, evidente che molti potrebbero essere i casi di *data breach* nel contesto scolastico. Non potendo fornire un elenco esaustivo dei possibili casi di violazione di dati, si presentano di seguito alcuni esempi di *data breach*, che devono servire da guida e orientamento per tutto il personale scolastico, con l'avvertenza che si tratta di alcuni tra gli esempi possibili.

**Esempi di *data breach***:

1. perdita, furto, sottrazione o copia non autorizzata di un documento cartaceo od informatico contenente dati personali;
2. perdita o furto di una *pen drive*, di un *notebook* o di qualunque altro *device* contenente datipersonali;
3. Erronea divulgazione di foto/documenti tramite internet;
4. Impossibilità di accedere ai dati per cause accidentali o per attacchi esterni (a causa di virus o *malware*, ad esempio);

5. Accesso non autorizzato a sistemi di didattica a distanza da parte di terzi;
6. Modifica non autorizzata o accidentale di dati personali presenti sul registro;
7. Perdita della riservatezza subita da sistemi utilizzati per la didattica a distanza;
8. Divulgazione non autorizzata dei dati personali.

**2 – CHE COSA DEVE FARE LA SCUOLA IN CASO DI VIOLAZIONE**

L'art. 33 del GDPR impone al **titolare** del trattamento (ovvero alla Scuola, rappresentata dal Dirigente scolastico) di **notificare all'autorità di controllo (Garante privacy)** la violazione di dati personali **entro 72 ore** dal momento in cui ne viene a conoscenza, a meno che sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche.

In caso di rischio elevato, oltre alla notifica, il **titolare** è tenuto a dare comunicazione della violazione all'interessato (art. 34 GDPR). Si intende per interessato qualsiasi persona fisica, identificata o identificabile, che abbia fornito dati personali alla scuola.

La valutazione dell'opportunità della comunicazione al Garante o agli interessati spetta al titolare del trattamento, sentito il parere del Responsabile Protezione Dati il quale nella valutazione del rischio si consulterà, se del caso, anche con l'Amministratore di Sistema.

**3 - COSA DEVE FARE IL PERSONALE DELLA SCUOLA IN CASO DI VIOLAZIONE**

La scuola ha il dovere di contenere i rischi connessi ad eventuali *data breach*, predisponendo **interventi tempestivi, adeguati e finalizzati a limitare ogni possibile conseguenza** per il caso in cui si verifichi una violazione dei dati personali.

Pertanto, un dipendente (docente o ATA), **nel caso in cui rilevi una possibile violazione dei dati personali**, deve:

1. **darne immediata comunicazione al Dirigente Scolastico** o – qualora il Dirigente non sia immediatamente raggiungibile – al Responsabile della Protezione dei Dati o all'Animatore Digitale o al team digitale, che informano immediatamente il Dirigente o il Responsabile della Protezione dei Dati;

A questo scopo si forniscono i seguenti riferimenti:
Euservice srl via Dante Alighieri, 12 - 00027 Roviano (RM) - P.IVA 08879271008
Email: rpd@euservice.it
PEC: info@pec.euservice.it
Email: Giovanni.gobbi@euservice.it

**4 - ATTIVITÀ SUCCESSIVE ALLA SEGNALAZIONE**

Il Dirigente scolastico, di concerto con il Responsabile della Protezione dei Dati ed altre eventuali figure di cui la scuola si avvale (Animatore Digitale, Amministratore del sistema) per la gestione della privacy, provvede tempestivamente ad:

1. effettuare una prima indagine interna;
2. a definire la gravità dell'eventuale violazione.

In particolare il Dirigente procede a identificare i possibili rischi derivanti dalla violazione e a definire qualunque azione da intraprendere per la loro minimizzazione.

**4.1 – ATTIVITÀ DEL DIRIGENTE SCOLASTICO**

Il Dirigente scolastico deve, nello specifico, valutare **l'opportunità o la necessità** di fare la comunicazione:

1. al Garante entro le 72 ore dalla conoscenza del fatto

2. ed, eventualmente, alle persone fisiche minacciate nei loro diritti dall'evento.

Per l'adozione di tale decisione devono essere coinvolti ed esprimere il proprio parere:

- il Responsabile della Protezione dei Dati.

Tuttavia la decisione finale è di competenza del Dirigente scolastico, che ne è il responsabile.

Ferma restando la responsabilità del titolare del trattamento, il Dirigente e i suoi consulenti in ogni caso si avvalgono delle indicazioni di "Auto valutazione per la notifica di una violazione dei dati personali" fornite dal Garante (https://servizi.gpdp.it/databreach/s/self-assessment).

**5 - LA COMUNICAZIONE AL GARANTE**

Qualora il Dirigente scolastico ritenga di dover fare la segnalazione al Garante, egli dovrà effettuarla entro le 72dalla venuta a conoscenza della violazione, salvo motivato ritardo.

La notifica della violazione al Garante deve avvenire secondo quanto ora stabilito dal Garante, come espressamente previsto al seguente link: https://servizi.gpdp.it/databreach/s/.

Il Dirigente scolastico, in quanto titolare del trattamento deve predisporre una relazione, che deve essere redatta seguendo le indicazioni stabilite dal Garante, che si rinvengono al seguente link: https://servizi.gpdp.it/databreach/s/.

La relazione deve essere firmata digitalmente dal Dirigente scolastico, titolare del trattamento; alla elaborazione della relazione è opportuno che partecipi attivamente anche il RPD.

**6 - IL REGISTRO DELLE VIOLAZIONI**

L'Istituto adotta il registro delle violazioni, che si allega alla presente procedura.

Ogni violazione, anche nel caso in cui non sia comunicata al Garante o agli interessati, dove essere annotata nel registro delleviolazioni, tenuto costantemente aggiornato dalla scuola.

In caso di mancato invio al Garante e agli interessati, nel registro delle violazioni viene sinteticamente annotata la ragione della mancata comunicazione.

Il Dirigente scolastico
Luigi Franco
Firma autografa sostituita a mezzo stampa
ai sensi dell'art. 3, comma 2, del D.lgs. n. 39/1993

Il Dirigente scolastico
Luigi Franco
Firma autografa sostituita a mezzo stampa
ai sensi dell'art. 3, comma 2, del D.lgs. n. 39/1993