Intestazione Istituto

Prot. N° _____ Data _____

Oggetto: procedura gestione violazione dati personali (data breach)

Il Regolamento Europeo 679/2016 (GDPR) impone al titolare del trattamento di dati personali la definizione delle misure tecniche ed organizzative atte a garantire la protezione dei dati personali trattati. Il dirigente scolastico, rappresentante legale dell'istituzione scolastica titolare del trattamento, per garantire le misure organizzative più idonee a tutelare i dati personali trattati ha definito le linee guida per la gestione delle violazioni privacy di cui il presente documento è un estratto con la sintesi delle procedure adottate per la gestione dei data breach.

Cosa è una violazione di dati personali (data breach)

All'articolo 4, punto 12, il regolamento 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".

Esempi di data breach:

- sottrazione o copia non autorizzata di un documento cartaceo od informatico contenente dati personali
- perdita o furto di una pen drive, di un notebook o di qualunque altro dispositivo contenente dati personali
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- 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
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali
- 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

Cosa deve fare l'amministrazione in caso di violazione

L'art. 33 del Regolamento Europeo 679/2016 (GDPR) impone al titolare del trattamento di notificare all'autorità di controllo (Garante privacy) la violazione di dati personali entro 72 ore dal momento in cui ne viene a conoscenza. L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche, qualora, poi, il rischio fosse elevato, allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all'interessato.

La valutazione dell'opportunità della comunicazione al Garante o agli interessati spetta al titolare del trattamento (nella persona del dirigente scolastico) sentito il parere del Responsabile Protezione Dati e di altre eventuali figure che forniscono servizi di assistenza e consulenza.

Cosa deve fare il personale della scuola in caso di violazione

Il contenimento dei rischi associati ad una violazione di dati personali è strettamente legato alla tempestività e all'adeguatezza degli interventi atti a limitare ogni possibile conseguenza. E' allora necessario che qualora un dipendente dell'amministrazione rilevi una possibile violazione dei dati personali ne dia immediata comunicazione al Dirigente Scolastico o, qualora esso non sia immediatamente disponibile, al Responsabile della Protezione dei Dati o ad altre eventuali figure che gestiscono i sistemi informatici o che forniscono servizi di assistenza e consulenza informatica e normativa in modo da consentire la massima tempestività di intervento.

A questo proposito forniamo i seguenti riferimenti:

Responsabile Protezione Dati:

< denominazione> ()

Email: _____ ()

tel. _____ ()

Attività successive alla segnalazione

Il Dirigente scolastico, di concerto con l'RPD ed altre eventuali figure tecniche o consulenziali di cui si avvale la scuola per la gestione della privacy e dei sistemi informatici, provvederà ad effettuare una prima indagine interna e a definire la gravità dell'eventuale violazione. In particolare procederà a identificare i possibili rischi derivanti dalla violazione e a definire qualunque azione da intraprendere per la loro minimizzazione. In questa fase il dirigente scolastico dovrà valutare l'opportunità o la necessità di fare la comunicazione al Garante, che dovrà intervenire entro le 72 ore dalla conoscenza del fatto, ed eventualmente alle persone fisiche minacciate nei loro diritti dall'evento. In merito alla scelta dovranno essere coinvolti ed esprimeranno il proprio parere il RPD ed eventuali altri consulenti informatico/normativi ma la decisione finale dovrà essere del dirigente scolastico che sarà responsabile in base al principio della responsabilizzazione.

La comunicazione al Garante

Qualora il dirigente scolastico ritenga di dover fare la segnalazione al Garante dovrà effettuarla entro le 72 dalla venuta a conoscenza della violazione salvo motivare opportunamente il ritardo. La notifica della violazione al Garante dovrà avvenire dalla casella PEC istituzionale dell'amministrazione e dovrà essere indirizzata a protocollo@pec.gpdp.it. La mail dovrà avere come oggetto **"notifica data breach"** e dovrà avere allegata una relazione effettuata sulla base del modello messo a disposizione dal Garante al link: https://www.garanteprivacy.it/documents/10160/0/Modello+notifica+Data+Breach.pdf/6d1fa433-88dc-2711-22ab-dd5d476abe74?version=1.1. La relazione dovrà essere firmata digitalmente dal dirigente scolastico, titolare del trattamento, ma è opportuno che alla sua redazione partecipi attivamente il RPD.

Il registro delle violazioni

La violazione, che sia o no comunicata al Garante o agli interessati, dovrà essere annotata nel registro delle violazioni che dovrà essere tenuto costantemente aggiornato dalla Segreteria.