



ISTITUTO COMPRENSIVO RENDE COMMENDA

Via Caduti di Nassirya 87036 RENDE (CS) Tel. 0984-463930

Mail: csic8ak00c@istruzione.it Pec: csic8ak00c@pec.istruzione.it

C.M. CSIC8AK00C – C.F.: 98094130782 –

Codice Univoco UFYJTE - Codice iPa istsc_csic8ak00c



Ministero dell'Istruzione e del Merito



FUTURA

LA SCUOLA PER L'ITALIA DI DOMANI



ISTITUTO COMPRENSIVO - "RENDE - COMMENDA"-RENDE
Prot. 0013528 del 01/10/2024
VII-5 (Uscita)

**AI DOCENTI ISTITUTO
AI GENITORI
AGLI STUDENTI
ALL'ANIMATORE DIGITALE
AL TEAM D'INNOVAZIONE E TECNICO
ALLA DSGA**

Oggetto: La gestione della violazione dati personali (data breach)

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 che non abbia dato il consenso.

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:

Dott.ssa Anna CIMA, e-mail anna.cima@privacyscuole.it

Il Dirigente Scolastico
Dott.ssa Simona SANSOSTI

*Il presente documento informatico è stato sottoscritto con firma digitale
(artt. 20 e 24 del d.lgs. 82/2005 CAD e ss. mm.ii.)*