ISTITUTO COMPRENSIVO STATALE VINCENZO MONTI

VIA DON BOLDORINI 2 - POLLENZA (MC) – 62010 – Tel/fax: 0733549800

Email:mcic817008@istruzione.it - mcic817008@pec.istruzione.it

Codice Fiscale: 80007300439 - Cod. Min.:MCIC817008

A tutto il Personale

e p.c. ai Genitori

Istituto Comprensivo "V. Monti" - Pollenza

Alle Bacheche Digitali

OGGETTO: Procedura di Data Breach- art.33 Regolamento UE n. 2016/679.

Con la presente si trasmette, per opportuna conoscenza, quanto emarginato in oggetto.

Si ricorda di consultare periodicamente l'Area aggiornata "PRIVACY" del Sito istituzionale.

IL DIRIGENTE SCOLASTICO

Catia Scattolini

PROCEDURA DI DATA BREACH

La gestione di Data Breach

Ai sensi dell'art. 33 del Regolamento (UE) n. 2016/679, il Titolare del trattamento, in caso sia consapevole di una violazione dei Dati personali trattati, è tenuto a informare l'Autorità di controllo (il Garante per la protezione dei dati personali, nel caso del territorio italiano) entro e non oltre le 72 ore successive all'avvenuta conoscenza della violazione.

Data Breach e potenziali scenari

Il GDPR definisce violazione dei dati personali o Data Breach "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" (art. 4, n. 12). Le indicazioni di cui alla presente sezione della Procedura valgono per qualsiasi tipologia di Dato personale. Eventi di Data Breach possono riguardare sia casi cui è connesso un rischio marginale (es. perdita di una chiavetta USB di un dipendente), che casi più critici di furto o perdita di intere basi dati, quali, a titolo esemplificativo, le banche dati gestite dal Titolare del trattamento. Nel caso si verificasse una delle casistiche riportate di seguito, o un analogo scenario, è fondamentale chiedersi se e quale tipo di Dati personali sono coinvolti nell'evento, e, di conseguenza, procedere alla segnalazione:

- furto o smarrimento di laptop, smartphone, tablet appartenenti alla scuola e contenenti Dati personali;

- furto o smarrimento di documenti cartacei contenenti Dati personali;

- furto o smarrimento di dispositivi portatili di archiviazione non criptati, come chiavette USB e hard disk esterni, contenenti Dati personali;

- perdita o modifica irreparabile di archivi contenenti Dati personali in formato cartaceo o digitale (ad esempio, a causa di una errata cancellazione o modifica dai sistemi o dagli archivi digitali aziendali che non possa essere ripristinata attraverso l'uso di un backup);

- diffusione impropria di Dati personali, per mezzo di:

- invio di e-mail contenente Dati personali al destinatario errato;
- invio di e-mail con un file contenente Dati personali allegato erroneamente;
- esportazione fraudolenta o errata di Dati personali.

Processo di gestione del Data Breach

Al fine di consentire una gestione efficace e tempestiva delle violazioni dei Dati personali, il Titolare del trattamento adotta un processo strutturato per la gestione dei casi di Data Breach che prevede:

- rilevazione e segnalazione del Data Breach;
- analisi del Data Breach;
- risposta e notifica del Data Breach;
- registrazione del Data Breach.

Rilevazione e segnalazione del Data Breach

La rilevazione e segnalazione del Data Breach è un obbligo per tutti i dipendenti e/o collaboratori del Titolare del trattamento. Nel caso in cui si verifichi uno degli eventi sopradescritti o in tutti gli altri casi in cui il soggetto che tratta dati personali sia consapevole di altri eventi potenzialmente rischiosi per i documenti e gli archivi, è tenuto a informare immediatamente il Dirigente Scolastico il quale provvede – senza indugio – a darne notizia al responsabile per la protezione dei dati personali (DPO).

Analisi del Data Breach

A seguito della rilevazione e/o segnalazione, il Dirigente Scolastico – sentito il Responsabile per la protezione dei dati personali - effettua una valutazione al fine di verificare che nell'incidente rilevato siano stati effettivamente violati Dati personali trattati dall'Istituto. La suddetta analisi è finalizzata alla raccolta ed identificazione di varie informazioni, inserite poi nel "Registro di Data breach". Nell'ambito di tale analisi, il Titolare del trattamento – con il supporto del DPO - identifica le azioni di prima risposta da intraprendere nell'immediato per contenere gli impatti della violazione dei Dati personali.

Risposta e notifica del Data Breach

La precedente fase di analisi fornisce al Titolare del trattamento gli strumenti necessari a identificare e valutare le conseguenze negative e gli impatti causati dalla violazione di Dati personali rilevata. Nel caso in cui dovesse risultare improbabile che il Data Breach presenti rischi per i diritti e le libertà degli interessati, la notifica all'Autorità Garante risulta essere non obbligatoria. Tale valutazione è condivisa con il DPO. Qualora al contrario dovesse risultare possibile che il Data Breach presenti rischi per i diritti e le libertà degli Interessati, il Dirigente Scolastico, con il supporto del DPO, procedere a predisporre la notifica all'Autorità Garante secondo il modello seguente:

https://www.garanteprivacy.it/documents/10160/0/Modello+notifica+Data+Breach.pdf/6d1fa433-88dc-2711-22ab-dd5d476abe74?version=2.0

Oltre a notificare il Data Breach all'Autorità Garante, il Titolare del trattamento è tenuto a valutare l'esigenza di procedere con la denuncia all'Autorità Giudiziaria competente, nonché con la notifica del Data Breach anche ai soggetti interessati i cui dati siano stati violati. Il Dirigente Scolastico, di concerto con il DPO, valuta di volta in volta, sulla base della tipologia e del numero di Interessati, il canale di comunicazione che appare più opportuno per trasmettere la notifica agli stessi.

L'Istituto adotta specifiche strategie per prevenire o minimizzare il verificarsi di Data Breach. In primo luogo, occorre che tutti gli Incaricati del Trattamento siano consapevoli dei Dati personali che trattano attraverso i propri strumenti (anche cartacei) e dispositivi o a cui hanno accesso tramite i sistemi del Titolare del trattamento. Gli stessi dovranno custodire tali Dati personali ed i relativi documenti con cura e in modo responsabile sia all'interno sia all'esterno della propria area di lavoro.