ISTITUTO COMPRENSIVO "GIOVANNI GABRIELI" MIRANO (VE)
SCUOLE DELL'INFANZIA – PRIMARIA – SECONDARIA I Grado
Sede Centrale: Via Paganini, 2/A - 30035 - MIRANO (VE)
Tel. 041/431407 - Cod. mecc. VEIC85600Q - email: veic85600q@istruzione.it - Cod. fisc. 90159650275
Posta cert.: veic85600q@pec.istruzione.it - www.icgabrielimirano.gov.it
Codice fatturazione elettronica **UFBP1E** – Codice IPA **istsc_veic85600q – Codice AOO : AOOICSGG**

Circ. n. 135

Mirano, 13 dicembre 2018

All'albo web

A tutto il personale
sede scolastica

OGGETTO: **PRIVACY – DATA BREACH (Violazione dei dati personali)**

Al fine di conoscere come affrontare la situazione per cui, per motivi accidentali (smarrimento di una chiavetta USB) o per fatto illecito (furto di un server), si viene a determinare una violazione del sistema informatico che comporta il rischio di cancellazione, modifica o divulgazione non autorizzata di dati, si forniscono le seguenti informazioni.

Una violazione dei dati personali (c.d. *data breach*) può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali ed immateriali alle persone fisiche coinvolte.

Alcuni esempi che si possono fare di questi danni sono: la perdita del controllo dei dati personali che li riguardano o la limitazione dei loro diritti, casi di discriminazione, furto o usurpazione d'identità, decifratura non autorizzata delle forme di pseudonimizzazione attuate, pregiudizio alla reputazione, perdita di riservatezza dei dati protetti da segreto professionale e d'ufficio o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Nel rispetto della normativa in materia di trattamento dei dati personali, garantendo in particolare l'aderenza ai principi e alle disposizioni contenute nel Regolamento UE 679/2016 (Considerando n. 85, 86, 87, 88 ed Artt. 33 e 34) e nella Guidelines on personal data breach notification under Regulation 2016/679 – article 29 data protection working party, si forniscono - con riferimento agli articoli del G.D.P.R. di riferimento - alcune utili definizioni.

DEFINIZIONI
Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4, punto 1).

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4, punto 2).

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia digitalizzato o meno, centralizzato, decentralizzato o ripartito in modo funzionale o geografico (art. 4, punto 6).

Titolare del trattamento (DS): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.

Data Protection Officer (DPO): la persona fisica individuata come Responsabile della protezione dei dati personali ai sensi del GDPR (in particolare artt. 37, 38, 39).

Autorizzato al trattamento: la persona fisica, espressamente designata, che opera sotto l'autorità del titolare del trattamento, con specifici compiti e funzioni connessi al trattamento dei dati personali (art. 4, punto 10).

Responsabile del trattamento (DSGA): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (art. 4, punto 8).

Violazione dei dati personali (c.d. 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, punto 12)
Per la gestione delle ipotesi di violazione dei dati personali (data breach) ai sensi del Regolamento UE 2016/679 (G.D.P.R.), all'interno della struttura si indica, di seguito, la

PROCEDURA.
Ogni operatore autorizzato a trattare i dati personali, qualora venga a conoscenza di un potenziale caso di data breach, avvisa tempestivamente il Titolare del trattamento (Dirigente Scolastico).
Quest'ultimo, valutato l'evento, se confermate le preoccupazioni di potenziale data breach, lo segnala tempestivamente al Data Protection Officer (DPO), dr.Giancarlo Favero.
Ai fini di una corretta classificazione dell'episodio, il D.P.O. utilizzerà lo schema di scenario di data breach, allegato alla presente circolare.
Pertanto, sulla scorta delle determinazioni raggiunte, il DPO predispone l'eventuale comunicazione all'Autorità Garante, a firma del titolare, da inviare senza ingiustificato ritardo e, ove possibile, **entro 72 ore**, da determinarsi dal momento in cui il titolare ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza della verificazione di un incidente di sicurezza che riguardi dati personali.
Oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo.
E' comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il titolare venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività di follow-up (c.d. notifica in fasi).
La scelta e le motivazioni che hanno portato a non notificare l'evento deve essere documentata a cura del D.P.O.

Nel caso in cui dal data breach possa derivare un rischio elevato per i diritti e le libertà delle persone, anche queste **devono essere informate senza ingiustificato ritardo**, al fine di consentire loro di prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione.

SCHEMA DI VALUTAZIONE DEGLI SCENARI
Al fine di eseguire la valutazione dell'obbligatorietà o meno della notifica all'Autorità Garante dei data breach e di supportare i soggetti coinvolti nella procedura, si allega apposita modulistica da utilizzare nel caso si dovessero verificare situazioni specifiche.

LA NECESSITA' DI DOCUMENTARE
Come accade per tutti i sistemi basati sul concetto di "rischio" e di "valutazione del rischio", la documentazione degli episodi che hanno determinato un danno (violazione dei dati – data breach) è fondamentale al fine di adottare precauzioni (tecniche o comportamentali) che possano scongiurare il verificarsi nuovamente di quell'episodio.

L'Art. 33 del G.D.P.R. pone l'attenzione su questa esigenza; il metodo migliore per adempiere a questa regola ma anche per poter comprovare, in caso di ispezione, tale adempimento consiste nella tenuta di un registro dei data breach a cura del **Responsabile del trattamento** di cui la scuola si è dotata (Registro previsto dal Garante con provvedimento 161 del 04 Aprile 2013).
Il registro deve contenere, per ciascun episodio, queste informazioni essenziali:
1. Dettagli relativi alla violazione (cause, luogo, tipologia di dati violati);
2. Effetti e conseguenze della violazione (*presunti*);
3. Piano di intervento predisposto dal Titolare;
4. Le motivazioni delle decisioni assunte a seguito del data breach.

Tutti coloro che incorrono in uno dei casi sopra citati, dovranno, senza alcun indugio, provvedere a darne comunicazione scritta al dirigente scolastico dettagliando quanto previsto ai punti 1 e 2 del comma precedente.

Il sito dell'istituzione Scolastica, in apposita pagina denominata G.D.P.R. raccoglie documentazione specifica .

- Allegato modello monitoraggio sicurezza

IL DIRIGENTE SCOLASTICO Reggente

Daniela MAZZA