OBIETTIVO

La presente procedura ha come obietto la gestione di eventuali violazioni dei dati personali *("Data Breach*"), ai sensi degli artt. 33-34 del Regolamento Europeo 2016/679 (di seguito anche "GDPR") ed in accordo con quanto previsto dalla Linea Guida del Gruppo Art. 29.

Ai sensi dell'art. 4 del GDPR, per violazione si deve intendere: "*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."*

In tale contesto, il Regolamento sancisce l'obbligo per il Titolare del trattamento di notificare tempestivamente l'avvenuta violazione dei dati personali all'autorità di controllo e, in casi determinati e con specifiche modalità, di procedere alla comunicazione direttamente agli interessati.
Il *Data Breach* può scaturire sia dall'interno che dall'esterno dell'Istituto scolastico e, qualora non affrontato tempestivamente e in maniera adeguata, può comportare pericoli significativi per la privacy degli interessati cui i dati si riferiscono (es. discriminazioni, furti di identità, perdite economiche, etc). Le violazioni più comuni sono quelle derivanti dall'errore umano. Si pensi alla consegna e/o alla comunicazione di documenti contenenti dati personali alla persona sbagliata (es. errore nell'invio di un'e-mail).

Secondo le linee guida del WP 29 le violazioni possono essere classificate in tre tipologie:

Tipologia di violazione	Evento/Minaccia
Violazione della riservatezza	Accesso o trattamento non autorizzato o illecito
	Divulgazione non autorizzata
Violazione dell'integrità	Modifica non autorizzata o accidentale
Violazione della disponibilità	Perdita o distruzione accidentale o illegale

A seconda dei casi poi, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché una qualsiasi combinazione delle stesse.

DESTINATARI

Sono destinatari della presente procedura tutti i soggetti che ruotano intorno ai trattamenti dati effettuati dall'Istituto Comprensivo Statale Via Bologna Bresso (nel seguito, Titolare del Trattamento) In particolare, a titolo esemplificativo e non esaustivo:
- Dirigente Scolastico
- DSGA
- Assistenti
- Personale ATA
- Personale docente
- Fornitori

CHI	chiunque ne venga a conoscenza (personale, collaboratori, fornitori, responsabili del trattamento, Titolare, utenti esterni, DPO, ecc.)
A CHI	al Titolare del trattamento interessato dall'incidente di sicurezza
QUANDO	appena ne viene a conoscenza
COME	utilizzando le vie più brevi (telefonicamente, di persona, via e-mail/pec)

APPLICAZIONE

Qualora uno dei soggetti destinatari della presente procedura ritenesse che si sia verificata una violazione dei dati personali, senza ingiustificato ritardo egli deve darne avviso all'Istituto Comprensivo Statale Via Bologna Bresso e al funzionario amministrativo in materia di privacy e trasparenza.
Questi ultimi, a loro volta, provvederanno a prendere immediatamente contatto con il Responsabile della Protezione Dati (RPD o DPO) che, alla data di stesura della presente revisione, è la società FRAREG S.r.l. nella persona dell'Ing. Stéphane Jean Michel Barbosa.
Nel caso in cui la violazione dei dati dovesse coinvolgere le infrastrutture informatiche e non solo il cartaceo, dovrà essere

informato anche il consulente di riferimento, nonché amministratore di sistema, opportunamente nominato.

Il Titolare del Trattamento, dunque, insieme alle sopra citate funzioni, al fine di valutare se la violazione può rappresentare un rischio per "i diritti e le libertà delle persone fisiche" (GDPR articolo 33), effettua un'analisi sull'evento, sulle possibili cause e sulle misure da adottare nell'immediato.

Qualora l'analisi effettuata da tali parti dovesse portare a definire che la violazione **non costituisca un rischio** per i diritti e le libertà delle persone fisiche, il Titolare del trattamento, su indicazione del DPO, può decidere di **non notificare** l'evento all'Autorità di controllo.
Deve in ogni caso registrare l'avvenuta violazione per mezzo di apposito registro (documento denominato "**18938-RG-00-IC Bologna Bresso _Registro Violazioni"**).

Qualora, invece, l'analisi effettuata dovesse portare a definire che la violazione **costituisca un rischio** per i diritti e libertà delle persone fisiche, il Titolare del trattamento con il supporto del Responsabile della Protezione Dati e di altre figure di volta in volta considerate, deve procedere tempestivamente (e **non oltre le 72 ore** da quando è venuto a conoscenza dell'evento) alla **notifica della violazione all'Autorità di controllo** e dunque al **Garante della Protezione dei dati personali**.

Al fine di verificare se la violazione occorsa possa rappresentare un rischio per i diritti e le libertà degli interessati, l'esercente le funzioni di Titolare del trattamento può avvalersi del supporto del tool messo a disposizione dal Garante per la Protezione dei dati personali e reperibile al seguente link https://servizi.gpdp.it/databreach/s/self-assessment.
Il tool supporterà il Titolare del trattamento nell'individuazione delle azioni da intraprendere a seguito di una violazione dei personali.
Una volta accertato che il *data breach* possa rappresentare un rischio per i diritti e libertà degli interessati, ovvero la violazione dei dati personali sia ritenuta complessa, il Titolare del trattamento è tenuto a notificare, una volta ricevuto anche il parere del Responsabile della Protezione Dati (RPD/DPO), l'avvenuta violazione di dati personali all'Autorità Garante nel rispetto dei termini di cui sopra. Il Titolare del trattamento dovrà inviare la comunicazione tramite l'apposita procedura telematica resa disponibile nel portale dei servizi online dell'Autorità, raggiungibile al seguente indirizzo https://servizi.gpdp.it/databreach/s/.

La notifica all'Autorità dovrà contenere le seguenti informazioni:

- **natura** della **violazione** di dati personali, tra cui, ove possibile, le **categorie** e numero approssimativo di **persone interessate**, **tipologie** e numero approssimativo di **dati personali** in questione;
- **nome** e **recapito** del **responsabile della protezione** dei dati o del **Titolare del trattamento**;
- **descrizione** delle **probabili conseguenze della violazione** dei dati personali;
- **descrizione** delle **misure adottate** o proposte da adottare **per affrontare la violazione** dei dati personali, tra cui, se del caso, misure per attenuarne i possibili effetti negativi;
- **se la notifica non è stata effettuate entro 72 ore, le ragioni per le quali non è stata presentata in precedenza.**

L'Autorità di Vigilanza dovrebbe trasmettere conferma scritta della ricevuta della notifica.
Ove necessario, potrebbero essere richieste ulteriori informazioni che dovranno essere fornite senza indebito ritardo.

Qualora la violazione subita sia suscettibile di comportare un rischio elevato per i diritti e le libertà degli interessati il Titolare del trattamento, con il supporto del RPD/DPO, predispone la comunicazione agli interessati. La comunicazione all'interessato deve descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali e avere ad oggetto almeno quanto segue:

- il nome e i dati di contatto del Responsabile della Protezione dei Dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrizione delle probabili conseguenze della violazione dei dati personali;
- descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Si sottolinea, in ogni caso, che la notifica agli interessati non è dovuta se questa "*comporta uno sforzo sproporzionato*" (GDPR articolo 34). In tal caso, sarà effettuata una comunicazione tramite il sito internet o altre fonti di comunicazione.
Una volta che è stato deciso che la violazione giustifica comunicazione ai soggetti interessati di dati, il GDPR richiede che ciò avvenga senza indebito ritardo.

Oltre ai punti richiesti dal GDPR, può essere opportuno offrire consulenza alla persona interessata per quanto riguarda le azioni che possono essere in grado di adottare per ridurre i rischi connessi con la violazione di dati personali.