ISTITUTO COMPRENSIVO STATALE-LANZO TORINESE
Prot. 0004501 del 25/10/2023
I-4 (Uscita)

ISTITUTO COMPRENSIVO DI LANZO TORINESE
SCUOLA DELL'INFANZIA, PRIMARIA E SECONDARIA I GRADO
Via Vittorio Veneto, 2 – 10074 LANZO TORINESE
TEL – FAX. 0123/29154 – 0123/320196
C.F. 92028660014 – C.U. UFLX9F
SITO WEB: www.iclanzotorinese.it E-MAIL: TOIC82600G@istruzione.it

PROCEDURA PER LA GESTIONE DEL DATA BREACH

AI SENSI DEL GDPR 2016/679, DELLE LINEE GUIDA DEL WP29 E DELLE INDICAZIONI FORNITE DAL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

PREMESSA INTRODUTTIVA

L'Istituto Comprensivo di Lanzo Torinese, quale Titolare del Trattamento ai sensi del Regolamento europeo 2016/679 (da qui in avanti GDPR), è tenuto a garantire la sicurezza dei dati personali trattati nell'ambito delle proprie attività e ad agire prontamente in caso di violazione dei dati stessi (come definito al punto 3).

L'Istituto pianifica e mette in atto procedure idonee a rilevare e limitare tempestivamente gli effettidi una violazione, valutare il rischio per le persone fisiche e stabilire se sia necessario o meno notificare la violazione all'autorità di controllo competente e comunicarla alle persone fisiche interessate, ove necessario.

1. SCOPO DELLA PROCEDURA

Il presente documento ha lo scopo di indicare a tutti i soggetti che operano presso la scuola le modalità di gestione di una violazione, anche solo potenzialmente ***data breach***, ovvero di un episodio di violazione di dati personali, nel rispetto dei principi e delle disposizioni contenute nel GDPR. Il presente documento è messo a disposizione di tutto il personale d'ateneo, attraverso la pubblicazione nella pagina intranet destinata ai servizi dell'UO Protezione Dati.

La procedura sintetizza le regole gestire nel migliore dei modi una violazione dei dati/*data breach*, sotto i diversi aspetti relativi a:

- Modalità e profili di segnalazione al Titolare;
- Valutazione dell'evento accaduto;
- Modalità e profili di segnalazione all'autorità Garante per la protezione dei dati personali (daqui in avanti Garante Privacy);
- Eventuale comunicazione agli interessati.

2. VIOLAZIONE DEI DATI PERSONALI

Una violazione dei dati personali (o data breach), ovvero una 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 del GDPR) può, se non affrontata in modo adeguato e tempestivo, provocare **danni fisici, materialio immateriali** alle persone fisiche, ad esempio perdita del controllo dei dati personali che liriguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Il data breach, o "violazione dei dati personali" nella traduzione italiana, è un concetto estremamente ampio.

Esso include certamente eventi in cui l'intervento malevolo di terzi è manifesto, ma comprende anche una serie di ipotesi riconducibili all'inosservanza di norme sulla sicurezza da parte del Titolare del trattamento. Tendenzialmente, il concetto di *data breach* viene a essere equiparato a quello di rilevante discontinuità nel normale funzionamento di un sistema informatico.

Rientra nella categoria dei *data breach* anche un incidente sulla sicurezza dal quale deriva una perdita di disponibilità dei dati non permanente, ma circoscritta a un limitato periodo temporale, (ad esempio la perdita di accesso temporanea ai dati), in quanto potrebbe comunque comportare un significativo impatto sui diritti e le libertà degli individui (ad es. un blackout elettrico che impedisca all'interessato di accedere ai propri dati).

Anche la violazione che comporta la perdita temporanea di disponibilità **dovrebbe essere documentata** (così come nel caso di perdita o distruzione permanenti di dati personali); l'indisponibilità di un dato personale causata dalla manutenzione programmata del sistema in corso,non può essere considerata una "violazione della sicurezza" ai sensi del GDPR.

Le violazioni di dati personali possono essere ricondotte ad una serie di eventi tra cui:

- Furto dei dati
- Distruzione dei dati
- Modifica dei dati
- Accesso non autorizzato ai dati
- Diffusione dei dati

Per gestire tali data breach, occorre seguire le disposizioni di seguito descritte.

3. SOGGETTI TENUTI ALL'OSSERVANZA DELLA PROCEDURA

La procedura si rivolge a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza dell'Istituto, quali i lavoratori dipendenti, nonché coloro che, a prescindere dall'inquadramento contrattuale in essere, abbiano accesso ai dati per garantire l'esecuzione delle prestazioni richieste.

La procedura si rivolge anche che agli esterni che a qualsiasi titolo vengano a conoscenza di una violazione riguardante l'Istituto

4. GESTIONE DEL DATA BREACH

Le violazioni di dati personali sono gestite operativamente dall'UO Protezione Dati dell'Area Trasparenza e Protezione Dati – Direzione Affari Istituzionali, sotto la supervisione del Responsabile della Protezione dei Dati (da qui in avanti DPO).

Ogni soggetto sia interno che esterno all'Istituto, qualora venga a conoscenza di un potenziale caso di *data breach che riguardi la scuola*, è tenuto ad informare tempestivamente il Titolare, compilando l'apposito modulo: **MODULO DI SEGNALAZIONE VIOLAZIONE/SOSPETTO DATA BREACH presente sul sito**

della scuola (www.iclanzotorinese.edu.it) e trasmettendolo via mail all'indirizzo toic82600g@istruzione.it **all'attenzione del Dirigente Scolastico.**

La segnalazione ricevuta sarà valutata in ordine a stabilire il possibile rischio per gli interessati e successivamente annotata nel **REGISTRO delle violazioni.**

Le violazioni sono classificabili in base a due livelli:

LIVELLO 1 La violazione sarà solo annotata sul registro delle violazioni conservato agli Atti della scuola

LIVELLO 2 La violazione sarà annotata sul registro delle violazioni e ne verrà data comunicazione al Garante della privacy

Il livello a cui attribuire ogni violazione e la conseguente procedura adottata saranno stabiliti in accordo tra il Dirigente Scolastico ed il DPO.

Appurato il rischio conseguente alla violazione, gli artt. 33 e 34 del GDPR indicano al Titolare i termini,le modalità, i contenuti e le deroghe della notifica e della comunicazione di *data breach*.

Pertanto, affinché la violazione dei dati personali sia gestita correttamente, è necessario seguire i seguenti step:

1) Identificazione della violazione ed avvio delle azioni correttive per gestire la violazione;
2) Indagine su quanto avvenuto e valutazione del rischio per gli interessati, con annotazione nell'apposito registro da parte del Titolare del trattamento. In particolare saranno indicati la data , il luogo e le cause della violazione, quali sono le banche dati violate, tipologia dei dati violati, effetti e conseguenze della violazione, piano di intervento e motivazioni.
3) Eventuale notifica all'Autorità del Garante tramite il modulo presente sul sito del Garante stesso;
4) Eventuale comunicazione agli interessati;
5) Documentazione della violazione indipendentemente dall'esito della valutazione.

5. RUOLO DEL DPO

In termini di documentazione delle violazioni, il Titolare del trattamento o il Responsabile del trattamento devono richiedere il parere del proprio DPO in merito alla struttura, all'impostazione eall'amministrazione di tale documentazione.

Il DPO svolge un *ruolo chiave* nell'assistenza alla prevenzione delle violazioni, fornendo consulenza e monitorando la conformità delle procedure e delle azioni poste in essere, nonché nel corso di notifica all'Autorità Garante e durante qualsiasi successiva indagine da parte della stessa.

Pertanto, l'Istituto informa tempestivamente il proprio DPO dell'esistenza di una violazione, coinvolgendolo durante la gestione delle violazioni ed il processo di notifica.