Procedura Data Breach

A. Definizioni

Violazione dei dati personali	
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;	
Violazione della riservatezza	accesso non autorizzato o accidentale ai dati
Violazione della disponibilità dei dati	distruzione dei dati o indisponibilità accidentale o non autorizzata
Violazione dell'integrità	modifica non autorizzata o accidentale dei dati

B. Sistemi

La violazione riguarda i dati personali a prescindere dal sistema su cui essi risiedono o sono conservati, compresi pc portabili, smartphone e tablet, di proprietà dell'ente.

C. Rilevazione

L'informazione relativa a una presunta violazione di dati personali può provenire da:

- Fonti esterne: cittadini, utenti dei servizi online, outsourcer, fornitori di servizi, ...
- Fonti interne: dipendenti, collaboratori

In entrambi i casi, l'informazione può essere acquisita dalla fonte in modo occasionale o a seguito di specifici controlli di cui alla lettera H.
I dipendenti che vengano a conoscenza di una presunta violazione di dati ne informano immediatamente il Dirigente Scolastico.

D. Valutazione

Il Dirigente Scolastico che sia stato informato di una presunta violazione di dati personali:

- verifica al più presto la veridicità dell'informazione considerando tra l'altro i seguenti aspetti:
    - l'informazione ha ragionevolmente riscontro positivo se essa è accompagnata da un dato personale che non dovrebbe essere nella disponibilità della fonte;
    - se l'informazione riguarda la sottrazione di credenziali di accesso, essa ha ragionevolmente riscontro positivo se contestualmente o in un breve lasso di tempo si riscontrano altre analoghe informazioni
- verifica al più presto, consultando il Responsabile della protezione dei dati, se la violazione presenta un rischio per i diritti e le libertà delle persone fisiche. In caso contrario, infatti, non è necessario procedere alla notifica. La verifica è effettuata considerando tra l'altro i seguenti aspetti:

    - nel caso di violazione della riservatezza, non vi è rischio se il dato personale è già pubblico o comunque nella disponibilità del pubblico;
    - nel caso di violazione della riservatezza, non vi è rischio se i dati sono crittati e la sicurezza della chiave non è compromessa;
    - nel caso di violazione della disponibilità del dato, non vi è rischio se è disponibile il backup ed è possibile ripristinare la situazione in un breve lasso di tempo.
- se la verifica di cui sopra ha esito positivo, effettua la notifica;
- adotta le misure per affrontare la violazione e per mitigare gli effetti negativi della stessa;
- verifica la necessità di informare della violazione gli interessati, anche allo scopo di mitigare eventuali effetti negativi della violazione attraverso la loro collaborazione. La comunicazione agli interessati non è richiesta se:
    - i dati violati sono cifrati e la sicurezza della chiave non è stata compromessa;
    - sono state adottate misure che scongiurano un rischio elevato per i diritti e le libertà degli interessati;
    - la comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
- compila il registro delle violazioni di dati di cui al punto H. (piattaforma)

E. Notifica

Quando la violazione presenta un rischio per i diritti e le libertà delle persone fisiche è necessario effettuare la notifica.
Il Dirigente Scolastico entro 72 ore dalla conoscenza della violazione effettua la notifica al Garante utilizzando l'apposito modulo disponibile sul sito dell'Autorità e fornendo tutte le informazioni richieste, per quanto disponibili.

F. Comunicazione agli interessati

Il Dirigente Scolastico, sentito in merito il Responsabile della protezione dei dati, valuta la necessità di effettuare la comunicazione agli interessati e in caso positivo sceglie le modalità più idonee

G. Registro delle violazioni dei dati

Il Dirigente Scolastico tiene il registro delle violazioni di dati personali compilando il registro disponibile sulla piattaforma Ckube.

H. Controlli

Si effettuano i seguenti controlli volti a monitorare i sistemi ed evidenziare eventuali violazioni di dati

- Alert del software Antivirus installato sui PC relativo alla compromissione del PC
- Alert del software Antivirus installato sui server relativo alla compromissione del server

- Alert del firewall relativo a tentativi di intrusione tramite intrusion detection and prevention systems (IDPS) o altri sistemi.