GDPR SCUOLA
LO STAFF TECNICO DEL DIRIGENTE

PROCEDURA DI RISPOSTA E COMUNICAZIONE DI UNA VIOLAZIONE DI DATI

(Gestione di Data Breach ai sensi del Regolamento Europeo 2016/679 nelle istituzioni scolastiche)

1. Campo d'applicazione, scopo e destinatari

Il presente documento si prefigge lo scopo di fornire a tutto il personale dell'I.C "Galileo Galilei" di Gravellona Toce, i principi generali e un modello di approccio per rispondere alle violazioni dei dati personali (data breach).

In questo documento sono sintetizzate le regole per garantire il rispetto dei principi esposti, e la realizzabilità tecnica e la sostenibilità organizzativa nella gestione del data breach.

La procedura definisce i principi e le azioni generali per gestire con successo la risposta a una violazione di dati e adempiere agli obblighi relativi alla notifica alle Autorità di controllo e ai singoli individui, come richiesto dal GDPR.

Tutto il personale che lavora o agisce per conto dell'istituto deve conoscere la procedura e seguirla in caso di violazione dei dati.

2. Documenti di Riferimento

- Il GDPR (Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio Europeo del 27 Aprile 2016 relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE)
- Codice della Privacy (D.Lgs 296/2003, come modificato dal D.L.gs 101/2018)
- Provvedimento del Garante del 30 luglio 2019 sulla notifica delle violazioni dei dati personali (doc. web n. 9126951).
- Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679

3. Definizioni

Le seguenti definizioni di termini utilizzati in questo documento sono tratte dall'articolo 4 del Regolamento Generale sulla Protezione dei Dati dell'Unione europea (o GDPR):

"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.

"Titolare del trattamento" dei dati: 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.

"Responsabile del trattamento" dei dati: una persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare.

“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.

“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.

“Autorità di controllo”: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR. In Italia è l’AUTORITA’ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (sede: Piazza di Montecitorio n. 121, Roma; sito www.gpdp.it - www.garanteprivacy.it; email garante@gpdp.it; telefono: 06.69677.1).

4. Le violazioni dei dati personali

Le violazioni dei dati personali possono avvenire per diverse ragioni, tra le quali, a titolo esemplificativo:

• Divulgazione di dati a persone non autorizzate

• Perdita o furto di dati o di strumenti nei quali i dati sono memorizzati

• Perdita o furto di documenti cartacei

• Illecito da parte di un dipendente (ad esempio: data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico)

• Accesso abusivo (ad esempio: data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite)

• Casi di pirateria informatica

• Banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo “owner”

• Virus o altri attacchi al sistema informatico o alla rete della scuola

• Violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate)

• Smarrimento di pc portatili, devices o attrezzature informatiche scolastiche

• Invio di email contenenti dati personali e/o particolari a erroneo destinatario

5. Procedura di risposta a una violazione dei dati

L'istituzione scolastica deve rispondere di qualsiasi sospetta/presunta violazione dei dati.

La scuola deve essere preparata a rispondere a una violazione 24 ore su 24, 7 giorni su 7, per tutto l'anno.

Le violazioni sono gestite dal titolare del trattamento (in persona del dirigente scolastico) sotto la supervisione del responsabile della protezione dei dati (RPD).

In caso di concreta, sospetta e/o presunta violazione dei dati, la stessa dovrà essere affrontata immediatamente e correttamente, da qualunque soggetto che ne è venuto a conoscenza, al fine di minimizzarne l'impatto e prevenire che si ripeta.

Chiunque venga a conoscenza di una sospetta/presunta violazione dei dati deve immediatamente comunicarla al Dirigente Scolastico.

Una volta segnalata una violazione dei dati, il Dirigente dovrà implementare quanto segue:

- Convalidare/assegnare un livello di urgenza alla violazione
- Assicurare che sia avviata, condotta, documentata e conclusa un'indagine corretta e imparziale (compresa l'informatica forense, se necessario)
- Identificare i requisiti per la risoluzione e monitorare la soluzione
- Coordinarsi con le autorità competenti, se necessario
- Assicurarsi che gli interessati siano adeguatamente informati, se necessario

Il dirigente dovrà quindi determinare se la violazione sia effettiva o meno.

La presente procedura di risposta a una violazione dei dati dovrà essere sempre avviata nel caso in cui chiunque (anche un soggetto terzo e estraneo alla scuola) si accorga di una sospetta/presunta o effettiva violazione e la comunichi all'Istituto scolastico.

6. Valutazione del responsabile della protezione dei dati

Qualora la violazione dei dati personali (o la sospetta violazione) riguardi i dati personali trattati dall'istituzione scolastica, il responsabile della protezione dei dati eseguirà le seguenti azioni:

1) Con l'istituto scolastico dovrà stabilire se la violazione dei dati vada segnalata all'Autorità di controllo.
2) Con l'istituto scolastico dovrà valutare il/i rischio/i per i diritti e le libertà dell'/ degli interessato/i in questione
3) Se è improbabile che la violazione dei dati comporti un rischio per i diritti e le libertà degli interessati, non è richiesta alcuna notifica (tuttavia, la violazione dei dati dovrà essere registrata).
4) L'Autorità di controllo dovrà essere informata senza indebito ritardo, e non oltre le 72 ore, qualora la violazione sia suscettibile di presentare un rischio per i diritti e le

libertà degli interessati colpiti (oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo).

7. **Notifica della violazione dei dati: comunicazione del titolare dei dati all'autorità di controllo**

Comunicazione al Garante della protezione dei dati personali:

Il dirigente scolastico invierà una comunicazione all'Autorità di controllo (Autorità Garante per la protezione dei dati personali), entro le 72 ore dall'avvenuta conoscenza.

Tale comunicazione dovrà includere quanto segue:

- Una descrizione della natura della violazione dei dati personali, comprese, ove possibile, le categorie e il numero approssimativo di interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione
- Il nome e le informazioni di contatto della scuola e del responsabile della protezione dei dati
- Una descrizione delle probabili conseguenze della violazione dei dati personali
- Una descrizione delle misure adottate (o di cui si propone l'adozione) da pare del titolare del trattamento per porre rimedio alla violazione e per gestire la medesima
- Qualsiasi informazione relativa alla violazione, compresa la documentazione raccolta

Il Garante della protezione dei dati personali ha predisposto apposito modulo per la segnalazione di un data beach reperibile al seguente link:

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9128501

Predisposizione di misure di contenimento dei danni causati dalla violazione dei dati:

Una volta accertata la presenza di una violazione, il dirigente, insieme al responsabile della protezione dei dati, dovrà stabilire:

- Se esistano azioni che possano limitare i danni che la violazione potrebbe causare

- Se sia necessario comunicare la violazione agli interessati

8. **Comunicazione di violazione dei dati personali: del titolare del trattamento dei dati all'interessato**

Il dirigente scolastico dovrà valutare il grado di rischio per i diritti e le libertà dell'interessato.

In caso di rischio elevato, gli interessati andranno informati senza indebito ritardo.

La comunicazione agli interessati dovrà essere scritta in un linguaggio chiaro e semplice.

Se, a causa dell'elevato numero di interessati, sarà sproporzionatamente difficile informare tutti i soggetti in questione, il dirigente dovrà adottare le misure necessarie per garantire che

le persone interessate siano informate utilizzando canali appropriati e pubblicamente disponibili.

9. Registro delle violazioni

Il dirigente scolastico (titolare del trattamento) deve documentare qualsiasi violazione di dati personali (anche quelle che non comportano l'obbligo di comunicazione al Garante o agli interessati) curando l'aggiornamento del registro delle violazioni, ai sensi dell'art. 33, comma 5 del GDPR.

10. Responsabilizzazione

Il personale scolastico che venga a conoscenza di una sospetta/presunta violazione dei dati deve immediatamente comunicarla al Dirigente Scolastico.

Qualsiasi individuo violi questa procedura sarà soggetto a misure disciplinari.

Potrebbe inoltre dover affrontare responsabilità civili o penali qualora le sue azioni violino la legge.