Ministero dell'Istruzione e del Merito
ISTITUTO COMPRENSIVO DI CASTELLAMONTE
VIA TRABUCCO 15 - 10081 CASTELLAMONTE (TO)
Codice Fiscale 92522690012 - Telefono 0124 515498

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'Istituto Comprensivo di Castellamonte, 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. n. 196/2003, come modificato dal D.lgs. n. 101/2018 e ss.mm.ii.)
- 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
- Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679, Versione 2.0, adottate il 28 marzo 2023, dal Comitato Europeo per la Protezione dei Dati (EDPB)

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 o del Referente Privacy designato) 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 e/o al Referente Privacy.

Una volta segnalata una violazione dei dati, il Dirigente/Referente 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/Referente 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).

5) Inoltre, se la violazione comporta **un rischio elevato** per i diritti e le libertà delle persone, il titolare deve comunicarla a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l'impatto.

6) A prescindere dalla notifica al Garante, il titolare del trattamento, documenta tutte le violazioni dei dati personali in un apposito registro (il registro delle violazioni).

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/Referente invierà una comunicazione all'Autorità di controllo (Autorità Garante per la protezione dei dati personali), entro le 72 ore dall'avvenuta conoscenza, decorrenti dal momento in cui il Titolare diventi consapevole della violazione dei dati.

Un Titolare del trattamento può considerarsi "a conoscenza" della violazione quando abbia conseguito un "ragionevole grado di certezza che la violazione si sia verificata" e che abbia causato una compromissione di dati personali.

La conoscenza dovrà considerarsi immediata in tutti quei casi in cui il Dirigente/Referente sia stato informato di una violazione, tramite segnalazione documentata di un terzo, ovvero abbia rilevato, direttamente e/o per il tramite del Responsabile del trattamento eventualmente designato, l'evento.

Diversamente, laddove la consapevolezza/conoscenza della violazione non possa dirsi immediata, si renderà necessario l'espletamento di apposite indagini volte ad appurare se la violazione abbia effettivamente avuto luogo.

In tali ipotesi, le indagini iniziali devono essere avviate dal Titolare del trattamento il prima possibile per permettere di stabilire rapidamente e con un ragionevole grado di certezza la sussistenza e la gravità della violazione.

Una volta che sia venuto a conoscenza di una violazione, il Dirigente è tenuto a valutare il rischio che tale violazione comporti per i diritti e le libertà delle persone fisiche coinvolte dal trattamento dei dati e a vagliare, caso per caso, la necessità o meno della notifica al Garante, nonché della comunicazione agli interessati.

Laddove, invece, risulti improbabile che la violazione dei dati personali possa generare rischi per i diritti e le libertà delle persone fisiche, il Dirigente può decidere di non inoltrare la notifica.

Tuttavia, se inviata, 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 la seguente pagine per la notifica di un data breach:

https://servizi.gpdp.it/databreach/s/

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

Una volta accertata la presenza di una violazione, il Dirigente/Referente, 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.

A seconda della probabilità e del grado del rischio rilevato, il Titolare del trattamento dovrà quindi:

1. Notificare la violazione dei dati personali all'Autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui sia venuto a conoscenza della stessa, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'Autorità di controllo non sia effettuata entro le 72 ore, è necessario che la stessa sia corredata dei motivi del ritardo;

2. Comunicare agli interessati la violazione dei dati personali senza ingiustificato ritardo, se la stessa sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche;

3. Riportare l'evento nel Registro delle violazioni (**questa attività dovrà essere compiuta a prescindere dal fatto che il Titolare del trattamento provveda o meno alla notifica e/o alla comunicazione dell'incidente di sicurezza**, e anche quando la violazione subita non presenti alcun rischio per i diritti e le libertà dei soggetti coinvolti - es.: compromissione di dati già pubblicamente disponibili).

Nell'eventualità in cui il Dirigente/Referente non entri immediatamente in possesso di tutti gli elementi utili per effettuare una descrizione completa ed esaustiva del *data breach* occorso, potrà procedere ad una notifica "per fasi", da attuarsi attraverso una prima e rapida notifica di alert (in occasione della quale l'Autorità verrà informata del contenuto solo parziale della segnalazione), seguita dalla comunicazione di tutte le informazioni aggiuntive acquisite, attraverso l'invio di successive notifiche integrative.

Inoltre, anche dopo aver completato le attività di notifica, il Dirigente/Referente ha comunque la facoltà di aggiornare l'Autorità di controllo, fornendo eventuali ulteriori dettagli di cui sia venuto a conoscenza nel tempo. Ciò a maggior ragione nel caso in cui, nel corso dell'indagine, venga appurato che l'incidente verificatosi sia stato contenuto e che non si sia effettivamente verificata alcuna violazione dei dati.

Non è prevista, del resto, alcuna sanzione per il caso in cui venga effettuata una segnalazione di un incidente che successivamente, non avendo effettivamente dato luogo ad alcuna violazione, si riveli essere un falso positivo.

Qualora la notifica all'Autorità di controllo non venga effettuata entro le 72 ore indicate dal GDPR, dovrà essere accompagnata dall'indicazione documentata dei motivi del ritardo.

Il GDPR prevede, altresì, la possibilità di effettuare una "notifica differita" dopo le 72 ore previste dall'articolo 33 nel caso in cui, ad esempio, si subiscano violazioni ripetute, ravvicinate e di simile natura che interessino un numero elevato di soggetti. In tal caso, il Titolare del trattamento è autorizzato ad eseguire un'unica "notifica aggregata" di tutte le violazioni occorse nel breve periodo di tempo (anche se superi le 72 ore), purché la notifica motivi le ragioni del ritardo.

Nel caso in cui si ometta di notificare una violazione dei dati all'Autorità di controllo, agli interessati, oppure a entrambi, nonostante siano soddisfatte le prescrizioni di cui agli artt. 33 e/o 34 del GDPR, l'Autorità Garante potrebbe adottare le misure correttive a sua disposizione, tra cui l'irrogazione di una sanzione amministrativa pecuniaria appropriata.

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

Il Dirigente/Referente 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, con il mezzo di comunicazione più efficace.

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/Referente (in nome e per conto della Scuola, 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 e/o al Referente Privacy.

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.