



Istituto Comprensivo Grosseto 1 "Alberto Manzi"

Via Corelli, 3 – 58100 Grosseto Tel. 0564 413622 Fax. 0564 427112

Cod. Meccanografico: gric830005

Codice Fiscale: 80003460534 - C.U.U.: UF83XE - codice IPA: istsc_gric830005

E-mail: gric830005@istruzione.it PEC: gric830005@pec.istruzione.it

www.icgrosseto1.edu.it

Prot. e data vedi segnatura

Atti interni

PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI (DATA BREACH)

1. Oggetto

La presente procedura disciplina le modalità di gestione delle violazioni di dati personali ("data breach") ai sensi degli artt. 33 e 34 del Regolamento (UE) 2016/679 (GDPR), all'interno dell'Istituzione scolastica.

La procedura definisce:

- obblighi di segnalazione interna;
- modalità di valutazione del rischio;
- criteri di notifica al Garante;
- criteri di comunicazione agli interessati;
- modalità di registrazione dell'evento;
- misure organizzative conseguenti.

2. Riferimenti normativi

- Regolamento (UE) 2016/679 (GDPR)
- D.lgs. 196/2003 e s.m.i.
- Linee guida del Comitato Europeo per la Protezione dei Dati (EDPB)
- Indicazioni operative del Garante per la protezione dei dati personali

3. Definizione di violazione di dati personali

Ai sensi dell'art. 4, punto 12 GDPR, per violazione di dati personali si intende: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, perdita, modifica, divulgazione non autorizzata o accesso ai dati personali trasmessi, conservati o comunque trattati.

Le violazioni possono riguardare:

- **Riservatezza** (es. divulgazione o pubblicazione non autorizzata);
- **Integrità** (es. modifica non autorizzata dei dati);
- **Disponibilità** (es. perdita, distruzione o indisponibilità dei dati).

4. Ambito di applicazione

La presente procedura si applica a:

- Dirigente Scolastico;
- DSGA;
- Personale docente e ATA;
- Responsabili esterni del trattamento;
- Responsabile della Protezione dei Dati (DPO).

5. Obbligo di segnalazione interna

Chiunque venga a conoscenza di una possibile violazione di dati personali è tenuto a:

1. Informare immediatamente il Dirigente Scolastico;
2. In caso di assenza, informare il DSGA;
3. Compilare il Modulo interno di segnalazione Data Breach;
4. Non adottare iniziative autonome non autorizzate.

La tempestività è elemento essenziale ai fini del rispetto del termine di 72 ore previsto dall'art. 33 GDPR.

6. Coinvolgimento del DPO

Il Dirigente Scolastico informa il Responsabile della Protezione dei Dati (DPO) senza ritardo e, comunque, entro 24 ore dalla conoscenza della presunta violazione.

Il DPO fornisce supporto e consulenza nella valutazione dell'evento, nella determinazione del livello di rischio e nella predisposizione dell'eventuale notifica al Garante e della comunicazione agli interessati.

Resta ferma la responsabilità decisionale del Titolare del trattamento in merito:

- alla qualificazione dell'evento come violazione;
- alla sussistenza dell'obbligo di notifica;
- alla comunicazione agli interessati;
- alle misure correttive da adottare.

L'eventuale mancato coinvolgimento del DPO deve essere motivato e annotato nel Registro delle violazioni.

7. Fase di prima valutazione

Il Dirigente, con il supporto del DPO e delle eventuali figure tecniche competenti:

- ricostruisce l'accaduto;
- individua tipologia di dati coinvolti;
- stima numero (anche approssimativo) di interessati;

- verifica durata dell'eventuale esposizione;
- adotta misure immediate di contenimento;
- richiede informazioni ai Responsabili esterni, se coinvolti.

8. Valutazione del rischio

Il Titolare valuta, in modo oggettivo e documentato:

- natura e categoria dei dati coinvolti;
- presenza di dati relativi a minori;
- facilità di identificazione degli interessati;
- probabilità e gravità delle conseguenze;
- numero di interessati;
- durata dell'esposizione.

Può essere utilizzato lo [strumento di autovalutazione](#) disponibile sul sito del Garante.

9. Notifica al Garante

Se la violazione è suscettibile di presentare un rischio per i diritti e le libertà delle persone fisiche:

- la notifica deve essere effettuata entro 72 ore dalla conoscenza del fatto;
- la notifica avviene esclusivamente tramite [procedura telematica online](#) sul sito del Garante per la protezione dei dati personali;
- qualora le informazioni non siano complete, la notifica può essere integrata successivamente.

In caso di ritardo, devono essere indicate le motivazioni.

10. Comunicazione agli interessati

Qualora la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare comunica l'evento agli interessati senza ingiustificato ritardo.

La comunicazione deve essere redatta in linguaggio chiaro e contenere:

- natura della violazione;
- possibili conseguenze;
- misure adottate;
- contatti del DPO.

11. Registro delle violazioni

Ogni violazione, notificata o meno, è annotata nel Registro interno delle violazioni.

Il registro contiene:

- data dell'evento;

- descrizione sintetica;
- categorie di dati coinvolti;
- numero stimato di interessati;
- misure adottate;
- decisioni assunte;
- eventuale notifica al Garante;
- eventuale comunicazione agli interessati.

Il Registro è custodito agli atti dell'Istituto sotto la responsabilità del Dirigente Scolastico.

12. Misure correttive e prevenzione

A seguito di ogni violazione o quasi-violazione, l'Istituto:

- aggiorna le procedure interne;
- rafforza eventuali misure tecniche;
- programma interventi formativi mirati;
- verifica l'adeguatezza delle misure organizzative.

13. Pubblicazione e diffusione

La presente procedura è pubblicata nella sezione "Privacy" del sito istituzionale ed è resa disponibile a tutto il personale.

Il Registro delle violazioni e il Modulo interno di segnalazione sono conservati agli atti e utilizzati esclusivamente per finalità interne.

14. Riesame

La procedura è soggetta a riesame:

- annuale;
- in caso di modifiche normative;
- a seguito di violazioni significative;
- su indicazione dell'Autorità Garante.

LA DIRIGENTE SCOLASTICA

Prof.ssa Barbara Bernardini

Documento informatico firmato digitalmente ai sensi del C.D. dell'Amministrazione Digitale e norme ad esso connesse