

ISTITUZIONE SCOLASTICA

LINEE GUIDA OPERATIVE

PER LA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI - DATA BREACH

Procedura operativa ai sensi degli artt. 33 e 34 del Regolamento (UE) 2016/679

OBIETTIVO

Fornire a tutto il personale una procedura chiara per riconoscere, contenere, segnalare e documentare tempestivamente ogni violazione, anche solo sospetta, dei dati personali.

Adottate con provvedimento del Dirigente scolastico n. 13817 del 25/09/2026

Versione 1.0 - 2026

Struttura del documento

- Parte I - Linee guida operative
- Parte II - Allegato A: Scheda di segnalazione immediata
- Parte III - Allegato B: Scheda di valutazione ex artt. 33 e 34 GDPR
- Parte IV - Allegato C: Casi pratici per il personale scolastico
- Parte V - Scheda rapida di pronto intervento

REGOLA ESSENZIALE

Il dipendente non deve stabilire autonomamente se un episodio debba essere notificato al Garante. Deve segnalare immediatamente l'evento. La qualificazione e la valutazione spettano al Titolare del trattamento, con il supporto del DPO.

PARTE I - LINEE GUIDA OPERATIVE

1. Finalità

Le presenti Linee guida disciplinano la gestione interna delle violazioni dei dati personali, con particolare attenzione ai trattamenti effettuati nell'ambito scolastico e ai dati riferiti a minori. La procedura è orientata alla tempestività, alla tracciabilità delle decisioni, alla conservazione delle evidenze e alla prevenzione della reiterazione dell'evento.

2. Che cos'è un data breach

È una violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato a dati personali trasmessi, conservati o comunque trattati.

- Riservatezza: i dati diventano accessibili a soggetti non autorizzati.
- Integrità: i dati vengono modificati o alterati senza autorizzazione.
- Disponibilità: i dati vengono persi, distrutti o diventano indisponibili.

3. Chi deve segnalare

Tutto il personale docente, educativo, amministrativo, tecnico e ausiliario che venga a conoscenza di una violazione o di una possibile violazione deve segnalarla senza ritardo. La segnalazione va effettuata anche quando l'errore è già stato corretto, non è certo che qualcuno abbia visualizzato i dati o l'evento appare di modesta entità.

NON ASPETTARE DI AVERE TUTTE LE INFORMAZIONI

La segnalazione iniziale deve essere immediata. Le informazioni mancanti possono essere acquisite successivamente.

4. Chi deve essere informato

- Dirigente scolastico;
- DSGA, quando l'evento riguarda attività amministrative o di segreteria;
- Responsabile della Protezione dei Dati (DPO), da coinvolgere senza ritardo.

5. Cosa fare nei primi minuti

- interrompere o limitare l'evento, se tecnicamente possibile;
- rimuovere documenti pubblicati erroneamente o correggere i destinatari;
- revocare accessi non autorizzati e, se necessario, bloccare credenziali/account;
- informare immediatamente Dirigente e DPO;
- preservare log, messaggi, documenti, screenshot e ogni altra evidenza;
- contattare tempestivamente il fornitore della piattaforma quando occorrono verifiche tecniche.

6. Cosa non fare

- non occultare o minimizzare l'evento;
- non cancellare log, e-mail o altre evidenze;
- non attendere l'esito di verifiche tecniche prima di segnalare;
- non decidere autonomamente che il fatto "non è grave";
- non comunicare informalmente l'accaduto a soggetti estranei alla gestione;
- non modificare retroattivamente le annotazioni già effettuate senza lasciare traccia dell'integrazione.

7. Acquisizione delle evidenze e dei log

Quando l'evento riguarda registro elettronico, piattaforme didattiche, posta elettronica, protocollo, cloud o altri applicativi, devono essere richiesti e conservati, ove disponibili, i dati tecnici necessari a ricostruire l'accaduto: orari, utenti abilitati, accessi, prese visione, aperture, download, modifiche dei permessi e ulteriori elementi utili. La richiesta deve essere tempestiva, anche in considerazione dei tempi di conservazione dei log.

8. Particolare attenzione ai minori e ai dati particolari

La valutazione deve essere particolarmente rigorosa quando l'evento riguarda minori, dati relativi alla salute o alla disabilità, PEI, GLO, PDP, diagnosi, certificazioni o altre informazioni idonee a rivelare condizioni di fragilità. Deve essere considerata anche la possibilità che il contesto consenta di inferire informazioni particolari pur in assenza di diagnosi o dati sanitari analitici.

9. Valutazione del rischio

Il Titolare, con il supporto del DPO, valuta il rischio tenendo conto congiuntamente delle circostanze concrete. La sola durata breve, il numero ridotto di destinatari o l'assenza di un danno già manifestato non sono, isolatamente, sufficienti a concludere la valutazione.

- natura e sensibilità dei dati;
- numero e caratteristiche degli interessati;
- minore età o vulnerabilità;
- durata dell'esposizione;
- numero dei destinatari potenziali ed effettivi;
- accessi, aperture e download rilevati;
- possibilità di ulteriore diffusione;
- misure di contenimento adottate;
- possibili conseguenze materiali e immateriali.

10. Art. 33 GDPR - Notifica al Garante

La violazione deve essere notificata all'Autorità di controllo senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui il Titolare ne è venuto a conoscenza, salvo che sia improbabile che la violazione

presenti un rischio per i diritti e le libertà delle persone fisiche. La decisione di non notificare deve essere specificamente motivata e documentata.

11. Art. 34 GDPR - Comunicazione agli interessati

La comunicazione agli interessati costituisce una valutazione distinta. Essa è richiesta quando la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, salvo le eccezioni previste dal GDPR. Il criterio del “rischio elevato” non deve essere utilizzato per decidere la notifica ex art. 33.

ATTENZIONE

Art. 33: la notifica può essere omessa solo quando è improbabile che la violazione presenti un rischio. Art. 34: la comunicazione agli interessati riguarda invece il rischio elevato. Le due valutazioni devono restare separate.

12. Registro delle violazioni

Ogni violazione deve essere documentata nel Registro delle violazioni dei dati personali, indipendentemente dalla notifica al Garante. Devono essere registrati i fatti, le conseguenze, le misure adottate e le ragioni delle decisioni assunte. Ogni integrazione successiva deve essere datata e tracciabile.

13. Analisi delle cause e misure correttive

La qualificazione come “errore umano” non esaurisce l’analisi. Occorre verificare se procedure, configurazioni, autorizzazioni, formazione o controlli possano essere migliorati. Le misure possono comprendere doppio controllo, revisione delle autorizzazioni, canali selettivi, pseudonimizzazione, cifratura, formazione, miglioramento del logging, revisione dei fornitori e audit.

14. Ruolo del DPO

Il DPO deve essere coinvolto senza ritardo. Supporta la qualificazione dell’evento, la valutazione del rischio, le decisioni ex artt. 33 e 34 e l’individuazione delle misure correttive. La decisione finale resta in capo al Titolare del trattamento; l’eventuale scelta di discostarsi dal parere del DPO deve essere motivata e documentata.

15. Flusso operativo

1. 1. BLOCCA - interrompi o limita l’evento.
2. 2. SEGNALE - informa immediatamente Dirigente e DPO.
3. 3. CONSERVA - preserva log, documenti ed evidenze.
4. 4. RICOSTRUISCI - acquisisci fatti, tempi, destinatari, accessi e download.
5. 5. VALUTA - analizza il rischio con il supporto del DPO.
6. 6. DECIDI - effettua separatamente la valutazione ex art. 33 e quella ex art. 34.
7. 7. REGISTRA - documenta evento e decisioni.
8. 8. CORREGGI - adotta e verifica le misure preventive.

PARTE II - ALLEGATO A

Scheda di segnalazione immediata di una possibile violazione dei dati personali

Istituzione scolastica:

Data e ora della segnalazione:

Nome, cognome e funzione del segnalante:

Data e ora in cui l'evento è stato rilevato:

Data e ora presunta dell'evento, se diversa:

Descrizione sintetica dell'accaduto:

Sistema/documento interessato:

- ☐ Registro elettronico
- ☐ E-mail/PEC
- ☐ Protocollo informatico
- ☐ Sito istituzionale
- ☐ Piattaforma didattica/cloud
- ☐ Documento cartaceo
- ☐ PC/dispositivo/supporto rimovibile
- ☐ Altro: _____

Dati potenzialmente coinvolti:

- ☐ Dati anagrafici/contatto
- ☐ Dati di minori
- ☐ Dati relativi alla salute/disabilità
- ☐ PEI/PDP/GLO/diagnosi/certificazioni
- ☐ Credenziali
- ☐ Dati economici
- ☐ Altro: _____

Soggetti che potrebbero aver avuto accesso / numero approssimativo:

☐ Sono già noti accessi o visualizzazioni: Sì / No / Non ancora verificato

Misure immediate adottate:

Evidenze disponibili:

- ☐ Log
- ☐ E-mail
- ☐ Screenshot
- ☐ Documento interessato
- ☐ Informazioni del fornitore
- ☐ Altro: _____

NON CANCELLARE LE EVIDENZE

Correggere l'errore non significa cancellare le tracce dell'accaduto. Preservare log, messaggi, documenti e informazioni tecniche.

Data/ora comunicazione al Dirigente:

Data/ora comunicazione al DPO:

Data/ora richiesta log, se necessaria:

Firma del segnalante:

PARTE III - ALLEGATO B

Scheda di valutazione della violazione - artt. 33 e 34 GDPR

Codice evento: DB-

Data/ora evento:

Data/ora scoperta:

Data/ora in cui il Titolare ha acquisito ragionevole certezza della violazione:

B.1 Ricostruzione

Descrizione dell'evento:

- ☐ Violazione della riservatezza
- ☐ Violazione dell'integrità
- ☐ Violazione della disponibilità

Causa e fattori organizzativi/tecnici che hanno contribuito:

B.2 Dati e interessati

- ☐ Dati comuni
- ☐ Dati di minori
- ☐ Categorie particolari ex art. 9
- ☐ Salute/disabilità
- ☐ PEI/PDP/GLO
- ☐ Informazioni che consentono inferenze su salute/fragilità
- ☐ Credenziali
- ☐ Altro: _____

Numero e categoria degli interessati:

- ☐ Sono coinvolti minori o soggetti vulnerabili: Sì / No / Da verificare

B.3 Estensione ed evidenze

Durata dell'evento:

Numero potenziale dei destinatari non autorizzati:

Numero di accessi/account effettivamente rilevati:

- ☐ Log acquisiti
- ☐ Prese visione verificate
- ☐ Aperture verificate
- ☐ Download verificati
- ☐ Inoltri verificati
- ☐ Accessi esterni verificati
- ☐ Evidenze non disponibili

Esito delle verifiche tecniche:

B.4 Contenimento

Misure adottate e relativo orario:

- ☐ La violazione è cessata: Sì / No / Parzialmente

B.5 Valutazione del rischio

- ☐ Perdita di riservatezza
- ☐ Discriminazione
- ☐ Danno reputazionale/sociale
- ☐ Perdita di controllo sui dati
- ☐ Furto/usurpazione d'identità
- ☐ Esposizione di salute/disabilità/fragilità
- ☐ Conseguenze scolastiche o relazionali
- ☐ Altre conseguenze: _____

Valutazione complessiva e motivazione:

B.6 Decisione ex art. 33 GDPR

- ☐ È improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche.

☐ Non può ritenersi improbabile la presenza di un rischio per i diritti e le libertà delle persone fisiche.

☐ NOTIFICA AL GARANTE

☐ NON NOTIFICA AL GARANTE

Motivazione analitica della decisione:

Scadenza delle 72 ore, ove applicabile:

B.7 Decisione autonoma ex art. 34 GDPR

☐ La violazione è suscettibile di presentare un rischio elevato: Sì / No

☐ COMUNICAZIONE AGLI INTERESSATI

☐ NON COMUNICAZIONE AGLI INTERESSATI

Motivazione:

B.8 Parere del DPO e decisione del Titolare

Data/ora coinvolgimento DPO:

Parere del DPO:

Decisione finale del Titolare e motivazione:

Firma del Dirigente/Titolare:

Firma del DPO per il parere reso:

B.9 Misure correttive e follow-up

Misure correttive individuate:

Responsabile e termine di attuazione:

Verifica successiva ed esito:

PARTE IV - ALLEGATO C

Casi pratici per il personale scolastico

Gli esempi indicano il comportamento immediato da tenere. Non stabiliscono automaticamente se l'evento debba essere notificato al Garante o comunicato agli interessati: tali decisioni richiedono la valutazione del caso concreto.

1. Convocazione GLO visibile alla classe

Scenario	Una convocazione contenente il nominativo di un alunno viene pubblicata per errore nella bacheca visibile ai genitori della classe.
Cosa fare subito	Rimuovere/correggere subito la visibilità; informare Dirigente e DPO; conservare le evidenze; richiedere i log di accesso, apertura e download; ricostruire durata e platea potenziale/effettiva; avviare la valutazione artt. 33 e 34.
Da evitare	Non concludere che l'evento sia irrilevante solo perché è durato poco o perché il documento non contiene una diagnosi esplicita.

2. PEI o PDP inviato al genitore sbagliato

Scenario	Un allegato destinato a una famiglia viene inviato a un altro genitore.
Cosa fare subito	Segnalare immediatamente; verificare contenuto e destinatario; chiedere la cancellazione e, ove possibile, conferma; conservare e-mail e riscontro; valutare natura dei dati e possibilità di ulteriore uso.
Da evitare	Non considerare la richiesta di cancellazione come prova automatica dell'assenza di rischio.

3. E-mail a più famiglie con indirizzi in CC

Scenario	Gli indirizzi dei genitori diventano reciprocamente visibili.
Cosa fare subito	Segnalare; individuare destinatari e contesto; verificare se dagli indirizzi o dal contenuto possano emergere ulteriori informazioni; documentare l'evento.
Da evitare	Non ignorare l'episodio con la motivazione che sono visibili "solo gli indirizzi e-mail".

4. Certificazione sanitaria al destinatario errato

Scenario	Una certificazione o altra documentazione sanitaria viene inviata a soggetto non autorizzato.
-----------------	---

Cosa fare subito

Attivare immediatamente la procedura; tentare il contenimento; coinvolgere DPO; verificare accesso/download e natura delle informazioni; procedere con particolare rigore alla valutazione del rischio.

Da evitare

Non attendere la fine della giornata o la risposta del destinatario prima di segnalare.

5. Documento con dati personali sul sito istituzionale**Scenario**

Un documento non destinato alla diffusione viene pubblicato online.

Cosa fare subito

Rimuovere tempestivamente; conservare copia ed evidenze; verificare durata, accessi e, ove pertinente, indicizzazione/cache; coinvolgere DPO e tecnico/fornitore.

Da evitare

Non limitarsi alla rimozione senza ricostruire l'esposizione.

6. Destinatari troppo ampi nel registro elettronico**Scenario**

Una comunicazione riservata è resa visibile a un gruppo più ampio di quello necessario.

Cosa fare subito

Correggere le autorizzazioni; acquisire log; distinguere chi poteva accedere da chi ha effettivamente acceduto; valutare i dati e il contesto.

Da evitare

Non cancellare la comunicazione prima di avere preservato le evidenze necessarie.

7. Perdita di notebook o chiavetta USB**Scenario**

Un dispositivo o supporto contenente dati scolastici viene smarrito o sottratto.

Cosa fare subito

Segnalare immediatamente; indicare dati presenti; verificare cifratura, password e possibilità di accesso; bloccare credenziali/sessioni ove necessario; valutare il rischio.

Da evitare

Non presumere che una password del dispositivo equivalga sempre a cifratura dei dati.

8. Account compromesso o phishing**Scenario**

Un dipendente inserisce le credenziali in un sito fraudolento o rileva accessi anomali.

Cosa fare subito

Cambiare credenziali, chiudere sessioni, attivare/verificare MFA; informare Dirigente, DPO e referente tecnico; acquisire log e verificare operazioni compiute dall'account.

Da evitare

Non limitarsi al cambio password senza verificare eventuali accessi o esfiltrazioni.

9. Fascicolo cartaceo lasciato accessibile

Scenario	Documentazione di un alunno rimane incustodita in un luogo accessibile a persone non autorizzate.
Cosa fare subito	Mettere in sicurezza il fascicolo; ricostruire luogo, durata e soggetti potenzialmente presenti; segnalare e documentare.
Da evitare	Non ritenere che il data breach riguardi soltanto sistemi informatici.

10. Destinatario dichiara di non aver aperto il file

Scenario	Dopo un invio errato, il destinatario riferisce di non aver aperto l'allegato e di averlo cancellato.
Cosa fare subito	Conservare il riscontro come elemento della valutazione; verificare, se possibile, ulteriori evidenze; documentare contenimento e circostanze.
Da evitare	Non chiudere automaticamente l'evento sulla sola base della dichiarazione.

11. Errore scoperto e corretto dallo stesso dipendente

Scenario	Il dipendente si accorge dell'errore pochi minuti dopo e lo corregge.
Cosa fare subito	Segnalare comunque; indicare tempi e azioni svolte; preservare le evidenze; consentire la valutazione formale.
Da evitare	Non omettere la segnalazione perché "ho già risolto".

12. Violazione comunicata da un fornitore

Scenario	Il gestore di una piattaforma informa la scuola di un incidente che può riguardare dati trattati per conto dell'Istituto.
Cosa fare subito	Acquisire senza ritardo natura dell'incidente, dati e interessati coinvolti, tempi, misure, log ed evidenze; coinvolgere DPO; svolgere la valutazione del Titolare.
Da evitare	Non presumere che gli adempimenti siano esclusivamente a carico del fornitore.

13. File condiviso con permessi "chiunque abbia il link"

Scenario	Un documento contenente dati personali viene condiviso mediante link con autorizzazioni eccessivamente ampie.
-----------------	---

Cosa fare subito

Limitare immediatamente i permessi; verificare cronologia accessi/download; conservare le evidenze; ricostruire chi abbia ricevuto il link e per quanto tempo sia rimasto utilizzabile.

Da evitare

Non considerare il link “privato” solo perché non è stato pubblicato sul sito.

14. Invio di elenco alunni con informazioni non necessarie**Scenario**

Un elenco destinato a un soggetto legittimato contiene colonne ulteriori e non necessarie.

Cosa fare subito

Segnalare se i dati eccedenti sono stati comunicati senza necessità; verificare destinatario, contenuto e possibilità di cancellazione; valutare la violazione e rafforzare la minimizzazione.

Da evitare

Non confondere la legittimità del destinatario con la legittimità di ogni dato trasmesso.

15. Cancellazione o indisponibilità accidentale di dati**Scenario**

Un errore tecnico o umano rende temporaneamente indisponibili dati necessari all'attività scolastica.

Cosa fare subito

Segnalare; verificare backup, durata e impatto; ripristinare in sicurezza; documentare causa e misure; valutare se la perdita di disponibilità incida sui diritti e libertà degli interessati.

Da evitare

Non limitare la nozione di data breach alla divulgazione di dati.

PARTE V - SCHEDA RAPIDA DI PRONTO INTERVENTO

È SUCCESSO QUALCOSA AI DATI PERSONALI?

Se hai un dubbio, segnala. Non devi stabilire tu se l'episodio debba essere notificato al Garante.

FASE	AZIONE	COSA FARE
1	BLOCCA	Interrompi o limita l'evento, senza distruggere le evidenze.
2	SEGNALA	Informa immediatamente il Dirigente e il DPO; il DSGA se competente.
3	CONSERVA	Salva log, e-mail, screenshot, documenti, orari e altre evidenze.
4	RICOSTRUISCI	Individua dati, interessati, destinatari, durata, accessi e download.
5	VALUTA	Il Titolare, con il DPO, valuta il rischio e documenta le ragioni.
6	ART. 33	Valuta autonomamente se ricorrono i presupposti per la notifica al Garante.
7	ART. 34	Valuta separatamente l'eventuale rischio elevato e la comunicazione agli interessati.
8	REGISTRA E CORREGGI	Aggiorna il Registro e adotta misure per evitare il ripetersi dell'evento.

CONTATTI DA COMPILARE

Dirigente scolastico: _____

DSGA: _____

DPO: _____

Referente tecnico / fornitore: _____

Approvazione e diffusione

Le presenti Linee guida, comprensive degli Allegati A, B e C e della Scheda rapida di pronto intervento, costituiscono riferimento operativo interno per il personale. Sono portate a conoscenza dei soggetti autorizzati al trattamento e sono oggetto di aggiornamento periodico e formazione.

Il Dirigente scolastico:

Data di adozione:
