protocollo n.0012267 del 20/10/2026

ISTITUTO COMPRENSIVO DI RUDIANO
25030 Rudiano BS - Via De Gasperi, n. 41 - TEL. 0307069017
C.F. 82002390175 C.M. BSIC86100R
email: bsic86100r@istruzione.it bsic86100r@pec.istruzione.it - internet: www.icrudiano.edu.it
codice univoco ufficio: UFJLBE
Scuole primarie e secondarie di primo grado di Rudiano, Roccafranca e Urago d'Oglio

Testo Revisionato e Aggiornato della Procedura (ottobre 2026)

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

(Ai sensi degli artt. 33 e 34 del Regolamento UE 2016/679 - GDPR, Linee Guida WP250 rev.01 e Linee Guida EDPB 01/2021)

Codice Procedura: PR-DB-2026_01

Proposta da: Responsabile della Protezione dei Dati (DPO/RPD) Vincenzi Gianfausto

Adottata da: Dirigente Scolastico (Rappresentante del Titolare) Bianco Gianfranco

Destinatari (Unità Organizzative):

- U.O. Personale Docente
- U.O. Personale Amministrativo (ATA - Segreteria e DSGA)
- U.O. Collaboratori Scolastici e Personale Ausiliario
- U.O. Collaboratori del DS e Staff di Direzione
- Componenti del Consiglio di Istituto

1. Oggetto e Ambito di Applicazione

La presente procedura definisce i ruoli, le tempistiche e i criteri per:

1. Rilevare e segnalare internamente qualsiasi incidente di sicurezza;
2. Valutare l'impatto e il rischio per i diritti e le libertà delle persone fisiche;
3. Gestire l'eventuale notifica all'Autorità Garante per la Protezione dei Dati Personali (entro 72 ore);
4. Gestire l'eventuale comunicazione agli interessati (senza ingiustificato ritardo);
5. Registrare l'evento nel *Registro delle Violazioni ex art. 33, par. 5, GDPR*;
6. Attuare e verificare le misure correttive e di contenimento.

2. Definizioni e Tipologie di Violazione

Ai sensi dell'art. 4, n. 12, del GDPR, per **violazione dei dati personali** si intende 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 trattati.

Documento informatico firmato digitalmente dal dirigente scolastico Prof.Bianco Gianfranco ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate

Le violazioni si distinguono in:

- **Violazione della Riservatezza:** Divulgazione di dati personali o accesso agli stessi da parte di soggetti non autorizzati (es. invio errato di PEI/diagnosi, credenziali compromesse).
- **Violazione dell'Integrità:** Alterazione o modifica non autorizzata o accidentale di dati (es. manomissione di voti, corruzione di registri o verbali).
- **Violazione della Disponibilità:** Perdita, distruzione o indisponibilità temporanea/permanente dell'accesso ai dati (es. attacco ransomware con cifratura file, rottura di supporto privo di backup, indisponibilità prolungata del registro lettronico durante scrutini).

Gestione Violazioni presso Fornitori Esterni / Cloud SaaS (Art. 28 GDPR):

- Qualora la violazione di sicurezza colpisca l'infrastruttura centrale di un fornitore cloud/SaaS (es. Registro Elettronico, Segreteria Cloud), il fornitore procede alla notifica formale al Garante per quanto di propria competenza e ne dà tempestiva notizia agli istituti scolastici (Titolari) a mezzo comunicazione diretta o avviso ufficiale centralizzato.
- La scuola acquisisce le risultanze tecniche fornite dal Responsabile e le iscrive nel proprio Registro delle Violazioni (art. 33, par. 5), verificando se l'evento richieda notifiche integrative specifiche o la comunicazione di misure di tutela agli interessati (es. reset forzato password, verifica accessi anomali).

3. Flusso Operativo delle Fasi di Gestione

Flusso Operativo di Gestione Data Breach (Swimlane Decisionale)

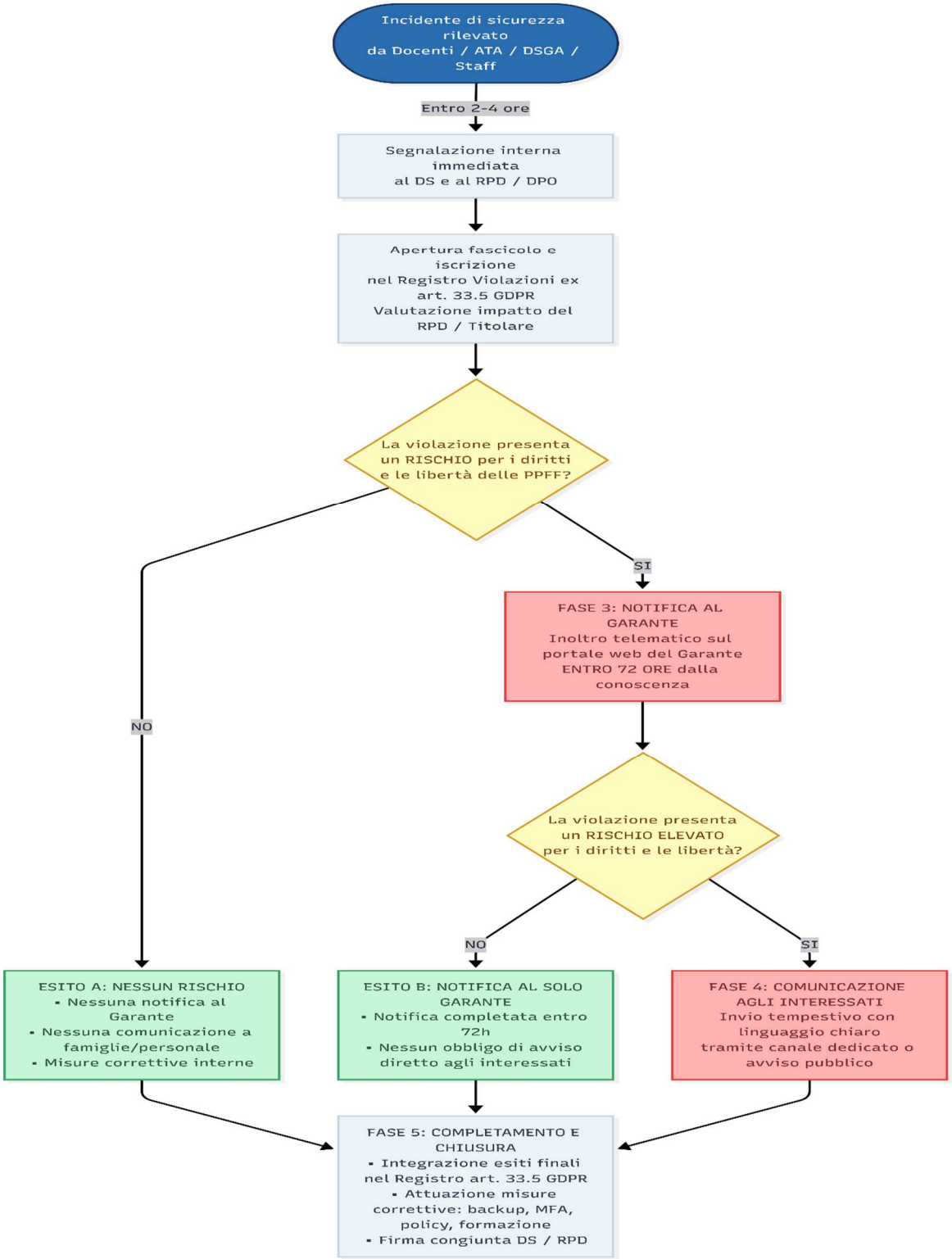


Tabella Operativa di Sintesi e Tempistiche

Fase	Azione Principale	Responsabile	Termine Perentorio	Strumento / Canale
1	**Segnalazione Interna**	Chiunque rilevi l'evento	**2 - 4 ore**	Email riservata al RPD / Segnalazione al DS
2	**Istruttoria e Registro**	RPD + DS + Ref. Tecnico	**Immediato**	Scheda Registro Violazioni ex art. 33.5 GDPR[cite: 2]
3	**Notifica all'Autorità**	Dirigente Scolastico	**Entro 72 ore** [cite: 2]	Servizio telematico web del Garante Privacy
4	**Avviso agli Interessati**	Dirigente Scolastico	**Senza ritardo** [cite: 2]	Canale diretto (email/bacheca RE) o avviso pubblico[cite: 2]
5	**Chiusura & Remediation**	DS + DSGA + RPD	**Post-incidente**	Verbale azioni correttive e piano formativo[cite: 2]

4. Dettaglio Operativo delle Fasi

Fase 1: Rilevamento e Segnalazione Interna Immediata

Chiunque all'interno dell'istituto rilevi un evento anomalo o incidente di sicurezza (es. furto PC/chiavetta USB, apertura di allegati ransomware/phishing, trasmissione massiva di email senza CCN, perdita fascicoli cartacei) è tenuto a **segnalarlo tempestivamente entro 2-4 ore** a:

- **Dirigente Scolastico** / **Collaboratori del DS** (per le sedi di plesso);
- **DSGA** (per l'area amministrativa e ausiliaria);
- **RPD/DPO** direttamente via email istituzionale (rpd@vincenzi.com).

Fase 2: Istruttoria, Iscrizione a Registro e Valutazione del Rischio

Il RPD, di concerto con il Titolare e con l'eventuale supporto degli Amministratori di Sistema/Referenti IT:

1. Istituisce e compila la prima sezione del **Registro delle Violazioni (art. 33, par. 5)** (data, sistemi coinvolti, categorie e numero approssimativo di interessati, natura dei dati);
2. Esegue la valutazione dell'impatto secondo i criteri di gravità e probabilità:
    - **Nessun Rischio:** Archiviazione dell'istruttoria a Registro senza adempimenti esterni.
    - **Rischio Presente:** Obbligo di notifica all'Autorità Garante entro 72 ore.
    - **Rischio Elevato:** Obbligo congiunto di notifica al Garante e comunicazione diretta agli interessati.

Fase 3: Notifica all'Autorità Garante per la Protezione dei Dati Personali

- La notifica deve essere trasmessa **entro 72 ore** dal momento in cui il Titolare è venuto a formale conoscenza dell'evento.
- **Modalità telematica:** La notifica viene inoltrata esclusivamente tramite il **servizio telematico per la notifica di data breach reso disponibile dall'Autorità Garante sul proprio portale web**.
- **Gestione Fornitori Esterni (Responsabili del Trattamento ex art. 28):** Qualora l'incidente avvenga sui server o applicativi di un fornitore cloud (es. Registro Elettronico, Segreteria Cloud), il fornitore ha l'obbligo contrattuale di informare la scuola *senza ingiustificato ritardo*. **Spetta sempre al Dirigente Scolastico (in qualità di Titolare) effettuare la notifica all'Autorità Garante**, indicando le risultanze tecniche fornite dal Responsabile.

Fase 4: Comunicazione della Violazione agli Interessati (Studenti, Famiglie, Personale)

- Scatta qualora la violazione presenti un **rischio elevato** (es. furto di database contenente dati sensibili/sanitari di minori, pubblicazione online di elenchi con password o dati giudiziari).
- La comunicazione è redatta in linguaggio chiaro e semplice, indicando la natura della violazione, i possibili rischi, le misure adottate dalla scuola e i contatti del RPD.
- **Esenzioni:** Non è dovuta se i dati erano resi incomprensibili (cifratura forte), se sono state adottate misure successive tali da neutralizzare il rischio elevato, o se richiederebbe sforzi sproporzionati (in tal caso si adotta un avviso pubblico sul sito istituzionale).

Fase 5: Chiusura Registro e Piano di Miglioramento

Il RPD e il Dirigente Scolastico:

- Completano l'annotazione sul Registro ex art. 33, par. 5, con le misure di contenimento adottate e i motivi delle decisioni prese;
- Pianificano le azioni correttive: ripristino da backup, revisione delle configurazioni di sicurezza (es. forzatura MFA, revisione permessi), richiami operativi o sessioni formative supplementari per il personale.

Tabella dei Casi Tipici e Orientamenti Decisionali

Evento / Incidente	Tipologia	Livello Rischio Tipico	Adempimenti Previsti
Invio massivo di email istituzionali visibili (omesso CCN) con soli indirizzi ordinari	Riservatezza	**BASSO**	• Iscrizione a Registro interno

Evento / Incidente	Tipologia	Livello Rischio Tipico	Adempimenti Previsti
			• Richiamo operativo / Nessuna notifica Garante
Invio accidentale a terzi di relazione clinica, PEI o verbale L. 104	Riservatezza (Dati Particolari)	**MEDIO-ALTO**	• Iscrizione a Registro • Notifica Garante (72h) • Valutazione comunicazione alla famiglia interessata
Infezione Ransomware con blocco PC di segreteria e ripristino da backup integro entro 4h (senza esfiltrazione)	Disponibilità (Temporanea)	**BASSO**	• Iscrizione a Registro • Nessuna notifica (integrità e riservatezza preservate)
Furto credenziali Registro Elettronico docente con alterazione di voti/note	Riservatezza / Integrità	**MEDIO-ALTO**	• Blocco immediato e reset credenziali • Iscrizione a Registro • Notifica Garante
Smarrimento chiavetta USB cifrata (BitLocker/AES) contenente documenti d'ufficio	Riservatezza	**NULLO / BASSO**	• Iscrizione a Registro • Nessuna notifica (dati incomprensibili ex art. 34.3.a)