Linee guida per la rilevazione e la gestione delle violazioni di dati personali (data breach)

Istituto Comprensivo "San Giulio"
Prot. 0007227 del 24/09/2026
I-4 (Uscita)

Il Regolamento (UE) 2016/679 (di seguito «Regolamento» o «GDPR») pone in capo al titolare del trattamento — l'Istituzione scolastica, rappresentata dal Dirigente scolastico — l'obbligo di notificare la violazione dei dati personali all'autorità di controllo competente e, in taluni casi, di comunicarla alle persone fisiche i cui dati sono stati interessati. Una violazione, se non affrontata in modo adeguato e tempestivo, può provocare alle persone fisiche danni fisici, materiali o immateriali: perdita del controllo dei propri dati, limitazione dei diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza di dati protetti da segreto professionale o altro danno economico o sociale significativo. Poiché nessuna misura tecnica od organizzativa può azzerare la probabilità di un incidente, il titolare è tenuto a dotarsi di un processo strutturato che consenta di rilevare tempestivamente le violazioni, contenerne gli effetti e assolvere gli obblighi di legge.

Le presenti linee guida sono redatte in coerenza con le Linee guida EDPB 9/2022 sulla notifica delle violazioni di dati personali (adottate il 28 marzo 2023, in aggiornamento delle Linee guida 01/2021 adottate il 14 dicembre 2021) e con la nota del Ministero dell'Istruzione n. 1248 del 28 luglio 2023, avente ad oggetto gli obblighi di notifica in caso di violazione dei dati personali.

1. Definizione di violazione di dati personali

L'art. 4, punto 12, del Regolamento definisce la violazione di dati personali come «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». Perché si possa porvi rimedio occorre anzitutto che il titolare e il personale autorizzato al trattamento siano in grado di riconoscerla. Si distinguono quattro modalità:

- **distruzione**: i dati non esistono più, o non esistono più in una forma che sia di qualche utilità per il titolare;
- **perdita**: i dati potrebbero esistere ancora, ma il titolare ne ha perso il controllo, l'accesso o il possesso;
- **divulgazione o accesso**: i dati sono divulgati a, o resi accessibili da, destinatari non autorizzati, ovvero trattati in altro modo in violazione del Regolamento;
- **modifica**: i dati sono stati alterati, corrotti o resi incompleti.

Sul piano degli effetti, le violazioni si classificano secondo i tre principi della sicurezza delle informazioni: **violazione della riservatezza** (divulgazione o accesso non autorizzati o accidentali), **violazione dell'integrità** (modifica non autorizzata o accidentale) e **violazione della disponibilità** (perdita, distruzione o inaccessibilità dei dati), anche in combinazione tra loro. La perdita di

disponibilità si ha, ad esempio, quando i dati vengono cancellati accidentalmente o da persona non autorizzata, oppure quando — nel caso di dati cifrati in modo sicuro — la chiave di decifratura viene perduta; se il titolare non è in grado di ripristinare l'accesso (ad esempio tramite backup), la perdita di disponibilità è considerata permanente. Rientra fra le violazioni della disponibilità anche l'interruzione significativa del servizio abituale (un attacco denial of service o, secondo le Linee guida 9/2022, persino una breve interruzione di corrente che impedisca, anche per pochi minuti, il funzionamento di un servizio di contatto con gli interessati).

Esempi ricorrenti in ambito scolastico

- sottrazione o copia non autorizzata di un documento, cartaceo o informatico, contenente dati personali;
- perdita o furto di una pen drive, di un notebook o di altro dispositivo contenente dati personali;
- impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware;
- dati e documenti cifrati da un ransomware, o cifrati dal titolare con una chiave non più in suo possesso;
- perdita o distruzione di dati a causa di incidenti, incendi o altre calamità;
- divulgazione non autorizzata di dati personali;
- e-mail inviata a più destinatari nei campi «a:» o «cc:», così da rendere visibili a ciascuno gli indirizzi altrui;
- indisponibilità prolungata di archivi (registro elettronico, segreteria digitale) a seguito di un attacco informatico.

2. Quando il titolare si considera «a conoscenza» della violazione

Il termine di 72 ore per la notifica decorre dal momento in cui il titolare acquisisce un ragionevole grado di certezza circa l'avvenuta violazione. In alcuni casi ciò è evidente fin dall'inizio; in altri occorre un breve accertamento per stabilire se i dati siano stati effettivamente compromessi. L'accento va posto sulla tempestività dell'indagine. Le Linee guida offrono alcuni esempi:

1. perdita di una chiave USB con dati non cifrati: spesso non è possibile accertare se terzi vi abbiano avuto accesso, ma poiché sussiste una ragionevole certezza della violazione della disponibilità, il caso va notificato; il titolare si considera «a conoscenza» dal momento in cui si accorge della perdita;
2. un terzo informa il titolare di aver ricevuto per errore dati personali e ne fornisce prova: il titolare è «a conoscenza» al momento della segnalazione;
3. il titolare rileva una possibile intrusione nella rete, verifica i sistemi e ottiene conferma della compromissione: è «a conoscenza» al momento della conferma;
4. un criminale informatico viola il sistema e chiede un riscatto: dopo aver verificato l'attacco, il titolare dispone di prova evidente ed è «a conoscenza»;

5. una persona segnala di aver ricevuto un'e-mail da chi si spaccia per il titolare, contenente dati veri: il titolare indaga, individua l'intrusione ed è «a conoscenza» in quel momento.

È quindi necessario che l'istituto disponga di procedure interne per rilevare e affrontare le violazioni: quando una violazione è rilevata, deve essere segnalata al livello di gestione appropriato, per essere trattata e, se del caso, notificata ai sensi dell'art. 33 e, se necessario, comunicata ai sensi dell'art. 34.

3. Quando notificare al Garante e quando comunicare agli interessati

L'art. 33, paragrafo 1, impone di notificare la violazione al Garante **senza ingiustificato ritardo e, ove possibile, entro 72 ore** dal momento in cui il titolare ne è venuto a conoscenza, **a meno che sia improbabile** che essa presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica non sia effettuata entro le 72 ore, deve essere corredata dei motivi del ritardo.

Quando la violazione è suscettibile di presentare un rischio **elevato**, all'obbligo di notifica al Garante si aggiunge, ai sensi dell'art. 34, quello di **comunicare la violazione agli interessati** senza ingiustificato ritardo. La soglia per la comunicazione agli interessati è più alta di quella per la notifica all'Autorità: non tutte le violazioni notificate al Garante vanno pertanto comunicate anche agli interessati, così da non arrecare loro disturbi non necessari.

4. La procedura interna in caso di presunta violazione

Chiunque — dipendente, collaboratore, alunno o genitore — rilevi una possibile violazione è tenuto a informarne **immediatamente il Dirigente scolastico** e, in caso di sua temporanea indisponibilità, il Responsabile della protezione dei dati (RPD/DPO) ovvero le altre figure, interne o esterne, che gestiscono i sistemi informatici e la sicurezza dei dati. La mancata segnalazione da parte del personale può dar luogo a provvedimenti disciplinari. I riferimenti di contatto sono riportati nella circolare al personale che accompagna le presenti linee guida.

Ricevuta la segnalazione, il Dirigente scolastico, con il supporto del RPD/DPO, del responsabile del trattamento e delle eventuali figure tecniche, procede senza indugio a: (a) contenere la violazione e limitarne gli effetti; (b) svolgere una prima indagine per accertare natura, cause ed estensione dell'evento; (c) classificare la violazione (riservatezza, integrità, disponibilità) e valutarne la gravità; (d) identificare i rischi per gli interessati e definire le misure di minimizzazione. Il processo deve restare proporzionato alla realtà scolastica, senza richiamare team o gruppi privacy che di fatto non sono presenti nell'istituto.

5. La decisione di notificare (o di non notificare) e la sua documentazione

Sulla base della valutazione, il Dirigente scolastico decide se ricorrano i presupposti per la notifica al Garante e per l'eventuale comunicazione agli interessati. Il RPD/DPO e gli altri consulenti esprimono il proprio parere, ma **la decisione finale spetta al titolare**, che ne risponde in forza del

principio di responsabilizzazione. Qualora il titolare decida in modo difforme dal parere del RPD/DPO, è opportuno che rediga un atto motivato che dia conto delle ragioni della scelta.

Merita particolare attenzione il caso in cui si decida di **non notificare** perché il rischio è ritenuto improbabile: in questa ipotesi il titolare deve comunque **documentare per iscritto la valutazione motivata** che ha condotto a non procedere, conservandola agli atti. La prassi applicativa più recente dell'Autorità mostra come una valutazione del rischio erronea o non documentata possa essa stessa formare oggetto di contestazione: la decisione di non notificare non è quindi un «non fare», bensì un adempimento che va tracciato e conservato al pari della notifica.

6. Modalità di notifica al Garante

Dal 1° luglio 2021 la notifica si effettua esclusivamente tramite la **procedura telematica** disponibile nel portale dei servizi online dell'Autorità, all'indirizzo https://servizi.gpdp.it/databreach/s/ (Provvedimento del Garante del 27 maggio 2021). Nella stessa pagina è disponibile un modello facsimile — utile per conoscere in anteprima i contenuti richiesti, ma non utilizzabile per l'invio — e uno **strumento di autovalutazione (self assessment)** che accompagna il titolare nell'individuazione delle azioni da intraprendere. Le istruzioni sono pubblicate all'indirizzo https://servizi.gpdp.it/databreach/s/istruzioni.

Ai sensi dell'art. 33, paragrafo 3, la notifica deve almeno:

- descrivere la natura della violazione, incluse, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni di dati coinvolti;
- indicare nome e dati di contatto del RPD/DPO o di altro punto di contatto presso cui ottenere informazioni;
- descrivere le probabili conseguenze della violazione;
- descrivere le misure adottate o proposte per porre rimedio alla violazione e, se del caso, per attenuarne gli effetti negativi.

Le **categorie di interessati** individuano i diversi tipi di persone fisiche coinvolte (tra cui, in ambito scolastico, minori e altri soggetti vulnerabili, personale, famiglie); le **categorie di registrazioni** individuano i diversi tipi di dati (dati sanitari, registri didattici, dettagli finanziari, e simili). Il considerando 85 chiarisce che, se i tipi di interessati o di dati rivelano un rischio di danno particolare, è importante che la notifica li indichi. L'indisponibilità di informazioni precise (ad esempio il numero esatto di interessati) non deve ritardare la notifica: il Regolamento consente approssimazioni e privilegia il tempestivo contenimento degli effetti rispetto alla fornitura di cifre esatte.

Notifica per fasi

Se, entro le 72 ore, il titolare non dispone ancora di tutte le informazioni — ipotesi frequente nelle violazioni informatiche complesse, che possono richiedere un'indagine forense — l'art. 33, paragrafo 4, consente una **notifica per fasi**: si trasmette una prima notifica con gli elementi disponibili, dichiarando all'Autorità di non disporre ancora di tutte le informazioni e che ulteriori dettagli

seguiranno senza ingiustificato ritardo; con l'Autorità si concordano modalità e tempistiche per le integrazioni. Ciò non impedisce di trasmettere ulteriori informazioni in qualsiasi momento. Se una successiva indagine dimostra che l'incidente è stato contenuto e che non vi è stata alcuna violazione, il titolare può informarne l'Autorità e l'evento può essere registrato come incidente non costituente violazione: **nessuna sanzione consegue** alla segnalazione di un incidente rivelatosi poi non costituente violazione.

Notifiche effettuate in ritardo e notifiche cumulative

La notifica oltre le 72 ore è ammessa purché corredata dei motivi del ritardo, ma non deve costituire la regola. Qualora il titolare subisca in poco tempo violazioni multiple e simili, che coinvolgono allo stesso modo un gran numero di interessati, può presentare una **notifica cumulativa** rappresentativa di tutte le violazioni, a condizione che riguardino il medesimo tipo di dati violati nello stesso modo in un lasso di tempo relativamente breve; se invece le violazioni riguardano tipi di dati diversi, violati in maniere diverse, si procede secondo l'iter ordinario, notificando ciascuna violazione. Le notifiche cumulative possono essere effettuate anche entro le 72 ore.

7. La comunicazione agli interessati

L'art. 34, paragrafo 1, impone la comunicazione agli interessati quando la violazione presenta un rischio elevato per i loro diritti e le loro libertà. La comunicazione deve avvenire «senza ingiustificato ritardo», cioè il prima possibile, con l'obiettivo principale di fornire agli interessati informazioni specifiche sulle misure che possono adottare per proteggersi. Ai sensi dell'art. 34, paragrafo 2, essa deve indicare almeno: la natura della violazione; il nome e i dati di contatto del RPD/DPO o altro punto di contatto; le probabili conseguenze; le misure adottate o proposte per porvi rimedio e attenuarne gli effetti. Il titolare dovrebbe fornire consigli concreti (ad esempio la reimpostazione delle credenziali compromesse).

Come contattare l'interessato

La comunicazione va di regola effettuata **direttamente** agli interessati, con **messaggi dedicati**, distinti da comunicazioni ordinarie (newsletter, circolari di routine), così da risultare chiara e trasparente. Sono idonei, ad esempio, la messaggistica diretta (e-mail, SMS), i banner o avvisi in evidenza sul sito, le comunicazioni postali. È essenziale scegliere il canale che massimizzi la probabilità di raggiungere effettivamente tutti gli interessati e, in particolare, **non utilizzare il medesimo canale compromesso dalla violazione** (ad esempio le caselle di posta oggetto dell'attacco), poiché ciò vanifica la comunicazione e può essere contestato dall'Autorità. Il considerando 88 consente, ove giustificato e su indicazione delle autorità incaricate dell'applicazione della legge, di ritardare la comunicazione per non pregiudicarne le indagini; decorso tale periodo, gli interessati vanno comunque informati. Se il titolare non dispone di dati di contatto sufficienti, informa l'interessato non appena ciò sia ragionevolmente possibile. Ove la comunicazione individuale richieda uno sforzo sproporzionato, si procede con una comunicazione pubblica o misura equivalente.

Casi in cui la comunicazione agli interessati non è richiesta (art. 34, par. 3)

- il titolare aveva applicato, prima della violazione, misure adeguate — in particolare la **cifratura allo stato dell'arte** o la tokenizzazione — che rendono i dati incomprensibili ai non autorizzati;
- il titolare ha adottato, subito dopo la violazione, misure che rendono **non più probabile** il concretizzarsi del rischio elevato;
- la comunicazione individuale richiederebbe uno **sforzo sproporzionato**: in tal caso si procede con una comunicazione pubblica o misura equivalente.

Anche in queste ipotesi il titolare deve poter dimostrare la sussistenza delle condizioni di esenzione; la valutazione va rivista nel tempo, poiché la situazione può mutare. L'Autorità può comunque richiedere la comunicazione agli interessati ove ritenga sussistente un rischio elevato.

8. Il registro delle violazioni

Ai sensi dell'art. 33, paragrafo 5, il titolare deve documentare **tutte** le violazioni di cui venga a conoscenza — comprese circostanze, conseguenze e provvedimenti adottati — **anche quando non siano notificate al Garante né comunicate agli interessati**. A tal fine l'istituto tiene costantemente aggiornato un **registro delle violazioni**, che per semplicità gestionale è integrato nel registro dei trattamenti. L'annotazione è dovuta anche in caso di mancata notifica: la sua omissione, in sede di contestazione, potrebbe aggravare la posizione del titolare, facendo presumere una volontà di occultamento dell'evento. La comunicazione al Garante, peraltro, può essere affrontata con serenità solo se l'istituto ha già assolto gli obblighi formali in materia di nomine e di documentazione privacy, che l'Autorità potrebbe richiedere in sede di verifica.

9. Rapporto con la disciplina sulla sicurezza delle reti (NIS2)

La notifica della violazione di dati personali al Garante (artt. 33 e 34 GDPR) va tenuta distinta dall'obbligo — introdotto dal recepimento della direttiva (UE) 2022/2555 con il D.Lgs. 138/2024 (NIS2) — di notificare gli **incidenti significativi** al CSIRT Italia, presso l'Agenzia per la Cybersicurezza Nazionale (ACN), secondo tempistiche proprie (preallarme entro 24 ore, notifica entro 72 ore, relazione entro un mese). Si tratta di due canali autonomi, con presupposti e destinatari diversi. L'obbligo NIS2 grava sui soli soggetti «essenziali» e «importanti» individuati dal decreto: le ordinarie istituzioni scolastiche non vi rientrano in via automatica e la loro eventuale inclusione dipende dai criteri e dalla registrazione presso l'ACN. Per la generalità delle scuole, pertanto, la gestione di una violazione di dati personali resta regolata dal solo canale GDPR verso il Garante; il canale NIS2/ACN rileva unicamente ove l'istituto rientri nel relativo perimetro.

10. Il ruolo del RPD/DPO e del responsabile del trattamento

Il RPD/DPO assiste il titolare nell'intero ciclo di gestione della violazione — rilevazione, valutazione, decisione sulla notifica e sulla comunicazione — e costituisce il punto di contatto indicato nella notifica e nelle comunicazioni. La responsabilità della decisione resta comunque del titolare.

Ove il trattamento sia affidato a un responsabile esterno (ad esempio il fornitore del registro elettronico o della piattaforma cloud), l'art. 28, paragrafo 3, lett. f), impone che il contratto preveda l'assistenza al titolare nell'assolvimento degli obblighi di cui agli artt. da 32 a 36. L'art. 33, paragrafo 2, stabilisce che il responsabile che venga a conoscenza di una violazione la notifichi al titolare **senza ingiustificato ritardo**; il responsabile non deve valutare la probabilità del rischio — valutazione che spetta al titolare — ma soltanto verificare l'avvenuta violazione e segnalarla.

Allegato A — Schema sintetico del processo di gestione

6. **Rilevazione** — chiunque rilevi una possibile violazione la segnala immediatamente al Dirigente scolastico (in subordine al RPD/DPO).
7. **Contenimento** — interventi immediati per arrestare la violazione e limitarne gli effetti.
8. **Indagine e classificazione** — accertamento di natura, cause ed estensione; classificazione (riservatezza / integrità / disponibilità).
9. **Valutazione del rischio** — determinazione del livello di rischio per i diritti e le libertà degli interessati, con il parere del RPD/DPO.
10. **Decisione** — notifica al Garante entro 72 ore se il rischio è probabile; comunicazione agli interessati se il rischio è elevato; in caso di mancata notifica, valutazione motivata documentata agli atti.
11. **Registrazione** — annotazione nel registro delle violazioni in ogni caso.

Allegato B — Esempi di violazioni e obblighi di notifica (elenco non esaustivo)

I seguenti esempi, tratti dalle Linee guida EDPB, aiutano a stabilire se e a chi effettuare la notifica e a distinguere tra rischio e rischio elevato per i diritti e le libertà delle persone fisiche.

Esempio	Notifica al Garante?	Comunicazione agli interessati?	Note
i. Backup di dati cifrati su chiave USB; la chiave viene rubata durante un'effrazione.	No, in linea di principio.	No.	Finché i dati restano cifrati allo stato dell'arte, esistono altri backup e la chiave di cifratura non è compromessa, può non trattarsi di violazione da notificare. Se la chiave viene poi compromessa, la notifica è necessaria.
ii. Servizio online oggetto di attacco informatico; vengono prelevati dati personali. Interessati in un solo Stato membro.	Sì, se vi sono probabili conseguenze per le persone fisiche.	Sì, secondo la natura dei dati e la gravità delle conseguenze.	Valutare l'estensione della compromissione e le misure di mitigazione.

Esempio	Notifica al Garante?	Comunicazione agli interessati?	Note
iii. Breve interruzione di corrente di alcuni minuti che impedisce l'operatività di un servizio di contatto con gli interessati.	No.	No.	Non è una violazione notificabile, ma resta un incidente registrabile ai sensi dell'art. 33, par. 5.
iv. Ransomware che cifra tutti i dati; nessun backup disponibile, dati non ripristinabili. L'indagine accerta la sola cifratura, senza altro malware.	Sì (perdita di disponibilità con probabili conseguenze).	Sì, in funzione della natura dei dati e degli effetti dell'indisponibilità.	Con backup ripristinabili in tempo utile la notifica non sarebbe stata necessaria.
v. Un interessato segnala di aver ricevuto l'estratto conto altrui; indagine breve (entro 24 ore) che rivela una potenziale carenza sistemica.	Sì.	Solo agli interessati coinvolti, in caso di rischio elevato.	Se emerge il coinvolgimento di più persone, informarne l'Autorità e comunicarlo agli altri interessati in caso di rischio elevato.
vi. Mercato online con clienti in più Stati membri; attacco a seguito del quale nomi utente, password e cronologia sono pubblicati online.	Sì, all'autorità capofila (trattamento transfrontaliero).	Sì (rischio elevato).	Adottare misure come il ripristino forzato delle password; considerare eventuali ulteriori obblighi di notifica.
vii. Società di hosting (responsabile del trattamento) individua un errore nel codice che controlla l'autorizzazione dell'utente.	Sì, quale responsabile, verso i titolari clienti, senza ingiustificato ritardo (che a loro volta valutano la notifica al Garante).	No, se non vi sono probabili rischi elevati per le persone fisiche.	Il responsabile deve considerare eventuali ulteriori obblighi di notifica. In assenza di prova di sfruttamento, potrebbe trattarsi di violazione solo da registrare.
viii. Cartelle cliniche di un ospedale indisponibili per 30 ore a causa di un attacco informatico.	Sì (possibile rischio elevato per la salute e la vita privata).	Sì, informare gli interessati.	Rischio elevato per categorie particolari di dati.
ix. Dati personali di un gran numero di studenti inviati per errore a una mailing list errata con oltre 1.000 destinatari.	Sì.	Sì, in base a portata, tipo di dati e gravità delle conseguenze.	Prestare attenzione alla presenza di categorie particolari e di minori.
x. E-mail di marketing inviata con i destinatari nei campi «a:» o «cc:», rendendo visibili gli indirizzi altrui.	Può essere obbligatoria se è coinvolto un numero elevato di persone, se sono rivelati dati particolari o se ricorrono altri fattori di rischio elevato.	Sì, nei casi rilevanti.	Può non essere necessaria se sono coinvolti pochi indirizzi e nessun dato particolare.

Il Dirigente Scolastico
Prof.ssa Katia Doddato
(
KATIA DODDATO
24.09.2026
09:52:50 CEST