Protocollo 0014178/2026 del 04/11/2026

Ministero dell'Istruzione
e del Merito

Istituto Comprensivo Statale "ALESSANDRO VOLTA"
Infanzia - Primaria - Secondaria I Grado
Via Volta, 13 - 20093 Cologno Monzese (MI) Tel. 02 25492649
Fax: 02 25492650 Cod. Mecc. MIIC8EH003 - C.F. 97632210155
E-mail:miic8eh003@istruzione.it
PEC: miic8eh003@pec.istruzione.it
Fatturazione Elettronica Codice Univoco: **UFR9XA**
Sito Web dell'istituto: www.scuolavolta.edu.it

All'Albo online e al sito web – sezione Privacy
Al personale docente e ATA

OGGETTO: Decreto di adozione della Procedura per la gestione delle violazioni dei dati personali (data breach) e del Registro delle violazioni – artt. 33 e 34 del Regolamento UE 2016/679

LA DIRIGENTE SCOLASTICA

VISTO il Regolamento UE 2016/679 del Parlamento europeo e del Consiglio (di seguito GDPR), e in particolare l'art. 4, n. 12, che definisce la violazione dei dati personali, l'art. 24 (responsabilità del titolare), l'art. 28 (responsabile del trattamento), l'art. 32 (sicurezza del trattamento), l'art. 33 (notifica di una violazione all'autorità di controllo), l'art. 34 (comunicazione di una violazione all'interessato) e l'art. 39 (compiti del responsabile della protezione dei dati);

VISTO il D.Lgs. 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali, come modificato dal D.Lgs. 10 agosto 2018, n. 101, e in particolare l'art. 2-quaterdecies;

VISTO l'art. 25 del D.Lgs. 30 marzo 2001, n. 165, che attribuisce al dirigente scolastico la legale rappresentanza dell'istituzione scolastica e autonomi poteri di direzione e di organizzazione;

VISTE le Linee guida EDPB 9/2022 sulla notifica delle violazioni dei dati personali ai sensi del GDPR (versione 2.0 adottata il 28 marzo 2023) e le Linee guida EDPB 01/2021 sugli esempi riguardanti la notifica delle violazioni dei dati personali (adottate il 14 dicembre 2021);

VISTA la nota del Ministero dell'Istruzione e del Merito – Direzione Generale per la progettazione organizzativa, l'innovazione dei processi amministrativi, la comunicazione e i contratti, Ufficio III – Protezione dei dati personali, prot. n. 1248 del 28 luglio 2023, recante "Obblighi di notifica in caso di violazione dei dati personali (c.d. data breach) – Novità introdotte dalla versione aggiornata delle Linee Guida n. 09/2022 del Comitato Europeo per la Protezione dei Dati", e le allegate "Linee guida per la gestione operativa dei data breach" del Ministero (versione agosto 2021), cui la presente Procedura si conforma per quanto compatibile con l'autonomia dell'istituzione scolastica, titolare dei trattamenti di propria competenza;

VISTO il provvedimento del Garante per la protezione dei dati personali n. 209 del 27 maggio 2021, che ha sostituito il provvedimento n. 157 del 30 luglio 2019 e ha istituito la procedura telematica per la notifica delle violazioni dei dati personali, operativa dal 1° luglio 2021;

VISTA la DPIA/TIA per l'adozione della piattaforma Google Workspace for Education (prot. n. 14145/2026 del 03/11/2026), che individua tra le misure di contenimento del rischio una procedura interna per la gestione degli incidenti che coinvolgono dati personali;

Documento informatico firmato digitalmente da INCORONATA NIGRO ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate

VISTE la circolare "Informative e istruzioni operative in materia di protezione dei dati personali" e le relative Linee guida per l'utilizzo sicuro delle piattaforme cloud dell'Istituto, che dispongono l'obbligo per il personale di segnalare senza ritardo ogni violazione, anche solo sospetta;

CONSIDERATO che l'Istituto tratta, anche con strumenti cloud, dati personali di minori e dati appartenenti a categorie particolari, per i quali una violazione può comportare rischi rilevanti per i diritti e le libertà degli interessati;

CONSIDERATO che il rispetto del termine di 72 ore previsto dall'art. 33 GDPR e l'obbligo di documentare ogni violazione (art. 33, par. 5, GDPR) richiedono ruoli, tempi e strumenti definiti in anticipo, operativi anche in caso di assenza o impedimento della Dirigente;

DECRETA

Art. 1 – Adozione. È adottata la "***Procedura per la gestione delle violazioni dei dati personali (data breach)***" dell'Istituto Comprensivo Statale "Alessandro Volta" di Cologno Monzese, allegata al presente decreto quale parte integrante e sostanziale (Allegato A), unitamente al Modulo di segnalazione interna (Allegato B), alla Scheda di valutazione della violazione (Allegato C), al Registro delle violazioni dei dati personali (Allegato D) e al Modello di comunicazione della violazione agli interessati (Allegato E).

Art. 2 – Sostituzione. In caso di assenza o impedimento della Dirigente Scolastica, le funzioni a questa attribuite dalla Procedura sono esercitate dalla prima collaboratrice, dott.ssa Maria Chiara Coronelli, che ne informa tempestivamente la Dirigente.

Art. 3 – Registro delle violazioni. È istituito il Registro delle violazioni dei dati personali di cui all'art. 33, par. 5, GDPR. Il Registro è tenuto dalla Dirigente Scolastica in un fascicolo riservato della Segreteria Digitale, accessibile alla sola Dirigente e alla DSGA.

Art. 4 – Obblighi del personale. Tutto il personale è tenuto a osservare la Procedura. L'omessa o ritardata segnalazione di una violazione di cui si sia venuti a conoscenza costituisce inosservanza delle disposizioni di servizio.

Art. 5 – Pubblicità e decorrenza. Il presente decreto, con i relativi allegati, è pubblicato all'Albo online e nella sezione Privacy del sito web istituzionale, è trasmesso al personale con le modalità previste per le circolari. Ha efficacia dalla data di pubblicazione.

LA DIRIGENTE SCOLASTICA

Prof.ssa Incoronata Nigro

Documento informatico firmato digitalmente ai sensi del c.d. Codice dell'Amministrazione Digitale e normativa connessa.

ALLEGATO A

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

1. Oggetto e finalità

La presente Procedura disciplina le modalità con cui l'Istituto, in qualità di titolare del trattamento, rileva, valuta, gestisce, notifica e documenta le violazioni dei dati personali. Si applica a tutti i trattamenti effettuati dall'Istituto, con qualunque strumento (registro elettronico e Segreteria Digitale, piattaforme ministeriali, Google Workspace for Education, dispositivi, archivi cartacei), e a tutto il personale docente e ATA, ai collaboratori e a chiunque operi per conto dell'Istituto.

2. Definizioni

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 trasmessi, conservati o comunque trattati (art. 4, n. 12, GDPR). Secondo le Linee guida EDPB, le violazioni si distinguono in tre tipologie, anche concorrenti tra loro:

Tipologia	Esempi frequenti in ambito scolastico
Violazione di riservatezza (accesso o divulgazione non autorizzati)	E-mail con dati di alunni inviata al destinatario sbagliato o con indirizzi in chiaro anziché in CCN; documento Drive condiviso con "Chiunque abbia il link"; annotazione con dati sanitari visibile alle famiglie; PEI o PDP lasciato incustodito; registro elettronico proiettato sulla LIM con dati di altri alunni; account compromesso tramite phishing; dati inseriti in strumenti di IA non autorizzati.
Violazione di integrità (modifica non autorizzata)	Valutazioni o assenze modificate da terzi che hanno usato credenziali altrui; documenti alterati da un collaboratore non autorizzato.
Violazione di disponibilità (perdita o indisponibilità)	Smarrimento o furto di PC, tablet, smartphone o chiavette contenenti dati; cancellazione accidentale di documenti; ransomware; indisponibilità prolungata di una piattaforma che impedisce servizi essenziali.

L'**indisponibilità temporanea** dei dati costituisce violazione se la mancanza di accesso può avere un impatto significativo sui diritti e sulle libertà degli interessati: va comunque documentata nel Registro, e la necessità di notifica si valuta caso per caso. Non costituisce violazione l'indisponibilità dovuta a un intervento di manutenzione programmata. La Procedura si applica allo stesso modo alle violazioni che riguardano **archivi cartacei**: distruzione accidentale (incendio, allagamento), distruzione per errore di originali senza copia, smarrimento, consegna a persona diversa dal destinatario, accesso non autorizzato, furto.

Non ogni incidente di sicurezza è una violazione di dati personali. Lo diventa quando coinvolge dati personali. Spetta al titolare, e non al singolo dipendente, stabilire se l'evento costituisca violazione: per questo **ogni evento, anche dubbio, va segnalato**.

3. Soggetti coinvolti e ruoli

Soggetto	Compiti
Dirigente Scolastica (titolare, in qualità di legale rappresentante)	Riceve le segnalazioni; dispone le misure di contenimento; valuta la violazione con il supporto del RPD; decide sulla notifica al Garante e sulla comunicazione agli interessati e vi provvede; tiene il Registro delle violazioni.
Prima collaboratrice, dott.ssa Maria Chiara Coronelli	In caso di assenza o impedimento della Dirigente esercita le funzioni di questa per l'intera procedura, compresa la notifica al Garante, e ne informa tempestivamente la Dirigente.

Soggetto	Compiti
Responsabile della Protezione dei Dati (RPD/DPO) **Ing. Antonio Vargiu –** **dpo@vargiuscuola.it**	È informato fin dal sospetto di violazione. Fornisce consulenza sulla valutazione del rischio, sulla notifica e sulla comunicazione agli interessati (art. 39 GDPR). Il parere è obbligatorio ma non vincolante ed è annotato nella Scheda di valutazione.
Amministratori di Google Workspace for Education **Animatore digitale e segreteria didattica –** **didattica@scuolavolta.edu.it** **dsga@scuolavolta.edu.it**	Su indicazione della Dirigente eseguono le misure tecniche di contenimento sulla piattaforma (sospensione account, reimpostazione password, revoca condivisioni, disconnessione dispositivi) e forniscono le informazioni tecniche disponibili (log di accesso e di condivisione).
Personale docente e ATA	Segnala immediatamente ogni violazione, anche solo sospetta; adotta le prime misure di contenimento indicate al par. 5; collabora all'istruttoria; non divulga notizie sull'evento.
Responsabili del trattamento esterni **(Spaggiari, Google e altri fornitori)**	Informano l'Istituto senza ingiustificato ritardo dopo essere venuti a conoscenza di una violazione (art. 33, par. 2, GDPR) e lo assistono negli adempimenti secondo il contratto o l'accordo sul trattamento dei dati.

4. Fase 1 – Segnalazione interna

- Chiunque venga a conoscenza di una violazione, anche solo sospetta, la segnala **immediatamente** alla Dirigente Scolastica, senza attendere di averne accertato la portata. Lo stesso vale per l'errore proprio e per gli eventi che appaiono di modesta entità o già risolti.
- La segnalazione si effettua per **e-mail istituzionale** alla Dirigente Scolastica (miic8eh003@istruzione.it e dirigente@scuolavolta.edu.it), con oggetto "URGENTE – SEGNALAZIONE POTENZIALE VIOLAZIONE DATI PERSONALI – RISERVATO", utilizzando preferibilmente il Modulo di segnalazione (Allegato B). Nei casi urgenti la segnalazione è anticipata per telefono alla Dirigente o, in sua assenza, alla prima collaboratrice, oppure alla segreteria (02 25492649).
- Se la segnalazione cade fuori dall'orario di servizio, nei giorni festivi o di sospensione delle attività, va comunque inviata per e-mail appena possibile. Il termine di 72 ore per la notifica decorre anche nei giorni non lavorativi.
- Nella segnalazione si riportano solo le informazioni necessarie a descrivere l'evento. Non si allegano i dati violati né si inoltrano i documenti coinvolti.
- La segnalazione non deve essere diffusa a colleghi, famiglie o terzi. Le comunicazioni agli interessati sono di esclusiva competenza della Dirigente.

5. Fase 2 – Contenimento immediato

Contestualmente alla segnalazione, e senza attendere istruzioni quando l'azione è semplice e non distrugge evidenze, chi rileva l'evento adotta le prime misure di contenimento. La Dirigente dispone le ulteriori misure, avvalendosi degli amministratori della piattaforma o dei fornitori.

Evento	Chi segnala fa subito	La Dirigente dispone
E-mail o documento inviato al destinatario errato	Chiede al destinatario di cancellarlo senza ulteriore diffusione e di confermarlo per iscritto; non reinvia lo stesso messaggio.	Acquisizione della conferma di cancellazione; valutazione del rischio.

Evento	Chi segnala fa subito	La Dirigente dispone
File su Drive condiviso per errore o con link aperto	Revoca subito la condivisione; annota da quando e fino a quando il file è stato accessibile.	Verifica dei log di accesso tramite gli amministratori.
Credenziali inserite in una pagina fraudolenta, account compromesso	Cambia subito la password; non cancella il messaggio sospetto.	Sospensione dell'account e revoca delle sessioni attive; verifica delle attività anomale; segnalazione al fornitore.
Dispositivo o supporto smarrito o rubato	Cambia le password degli account usati sul dispositivo; in caso di furto, sporge denuncia.	Disconnessione o cancellazione da remoto del dispositivo, ove possibile; acquisizione della copia della denuncia.
Accessi, modifiche o cancellazioni anomale su registro elettronico o Segreteria Digitale	Non corregge i dati prima di aver segnalato; annota quanto osservato.	Richiesta di assistenza e di estrazione dei log a Spaggiari; ripristino dei dati corretti.
Documenti cartacei smarriti, sottratti o lasciati accessibili	Recupera e mette al sicuro i documenti, se possibile; annota luogo e durata dell'esposizione.	Ricognizione dei documenti coinvolti; valutazione del rischio.

6. Fase 3 – Istruttoria e valutazione del rischio

Ricevuta la segnalazione, la Dirigente avvia senza ritardo l'istruttoria, coinvolgendo il RPD e, ove servano informazioni tecniche, gli amministratori della piattaforma o il fornitore interessato. Entro 24 ore dalla segnalazione, ove possibile, si compila la Scheda di valutazione (Allegato C). Il titolare si considera venuto a conoscenza della violazione quando ha un ragionevole grado di certezza che si sia verificato un incidente di sicurezza che ha compromesso dati personali. La fase di accertamento deve comunque essere breve, avviata il prima possibile e quanto più dettagliata possibile. La conoscenza è da considerarsi **immediata** quando la violazione è rilevata direttamente dal personale o dal responsabile del trattamento oppure è segnalata da un terzo con elementi documentati (ad esempio, chi ha ricevuto per errore dati di altri e ne fornisce prova). In caso di smarrimento di un supporto con dati non cifrati si presume che un accesso non autorizzato possa essersi verificato.

La valutazione del rischio per i diritti e le libertà degli interessati considera, secondo le Linee guida EDPB 9/2022:

– il **tipo di violazione** (riservatezza, integrità, disponibilità);

– la **natura e la delicatezza dei dati**. Il rischio è più elevato per i dati appartenenti a categorie particolari (salute, disabilità, DSA e BES), per i dati relativi a situazioni familiari o a provvedimenti disciplinari e per le credenziali di accesso;

– il **volume dei dati** e il **numero di interessati** coinvolti;

– la **facilità di identificazione** degli interessati;

– la **gravità e la durata delle possibili conseguenze** (discriminazione, danno reputazionale, pregiudizio psicologico, furto d'identità, perdita di controllo sui dati);

– le **caratteristiche degli interessati**. Gli alunni minorenni sono soggetti vulnerabili, e ciò incide in senso aggravante sulla valutazione;

– le **caratteristiche del titolare**: un'istituzione scolastica tratta abitualmente dati di minori e dati relativi alla salute e all'inclusione, il che richiede particolare cautela;

– le **conseguenze secondarie** della violazione, che possono incidere significativamente sulla vita degli interessati anche a distanza di tempo;

– le **misure già in essere o adottate subito** (ad esempio cifratura, cancellazione confermata dal destinatario affidabile, revoca tempestiva dell'accesso senza evidenze di consultazione). La cifratura esclude il rischio solo se è **robusta** e la chiave o la password non sono state compromesse.

All'esito, la violazione è classificata come segue:

Esito	Quando	Adempimenti
Rischio improbabile	Il rischio per gli interessati è improbabile (ad esempio, dati cifrati con chiave non compromessa; e-mail inviata per errore a un dipendente dell'Istituto che ne ha confermato la cancellazione).	Annotazione nel Registro con la motivazione della mancata notifica.
Rischio	La violazione può comportare un rischio per i diritti e le libertà degli interessati.	Annotazione nel Registro e **notifica al Garante** entro 72 ore.
Rischio elevato	La violazione può comportare un rischio elevato (ad esempio, divulgazione di dati sanitari o relativi alla disabilità di alunni; accesso di terzi a un account con dati di molti interessati).	Annotazione nel Registro, **notifica al Garante** entro 72 ore e **comunicazione agli interessati** senza ingiustificato ritardo.

In caso di dubbio tra due livelli si adotta, di norma, quello più cautelativo. Il parere del RPD e le ragioni della decisione sono annotati nella Scheda di valutazione.

7. Fase 4 – Notifica al Garante

- La notifica è effettuata dalla Dirigente o, in sua assenza, dalla prima collaboratrice, **senza ingiustificato ritardo e, ove possibile, entro 72 ore** dal momento in cui l'Istituto è venuto a conoscenza della violazione (art. 33, par. 1, GDPR).
- La notifica si invia esclusivamente mediante la **procedura telematica** disponibile sul portale dei servizi online del Garante (https://servizi.gpdp.it/databreach/s/). Sul sito del Garante sono disponibili un modello facsimile, utile per predisporre i contenuti ma non utilizzabile per l'invio, e uno strumento di autovalutazione.
- La notifica contiene almeno: la natura della violazione, con le categorie e il numero approssimativo di interessati e di registrazioni coinvolte; il nome e i dati di contatto del RPD; le probabili conseguenze; le misure adottate o proposte per porvi rimedio e attenuarne gli effetti (art. 33, par. 3, GDPR).
- Se non è possibile fornire subito tutte le informazioni, la notifica si effettua comunque nei termini. Si indica in prima battuta un numero **approssimativo** di interessati e di dati, poi precisato dopo gli accertamenti, e la notifica si integra successivamente **in fasi** (art. 33, par. 4, GDPR).
- La notifica effettuata oltre le 72 ore è corredata dei **motivi del ritardo**, documentati (art. 33, par. 1, GDPR). In caso di violazioni ripetute, ravvicinate e di natura simile che interessino numerosi soggetti, può essere effettuata un'unica **notifica aggregata**, motivando l'eventuale superamento del termine.
- Nel dubbio si notifica. Se l'istruttoria successiva accerta che non si è verificata alcuna violazione, se ne informa il Garante con una notifica integrativa e l'evento è annotato nel Registro come **falso positivo**: secondo le Linee guida EDPB, la notifica di un incidente che si riveli non essere una violazione non comporta sanzioni.

- Il momento in cui l'Istituto è venuto a conoscenza della violazione deve essere **dimostrabile**: data e ora si annotano nella Scheda di valutazione, perché da lì decorrono le 72 ore. Tutte le attività di scoperta e di gestione dell'incidente sono documentate in modo tracciabile.
- La ricevuta della notifica e le eventuali integrazioni sono conservate nel fascicolo riservato della violazione e annotate nel Registro.

8. Fase 5 – Comunicazione agli interessati

- Quando la violazione è suscettibile di presentare un **rischio elevato**, la Dirigente la comunica agli interessati senza ingiustificato ritardo (art. 34, par. 1, GDPR). Per gli alunni minorenni la comunicazione è rivolta a chi esercita la responsabilità genitoriale.
- La comunicazione è redatta in linguaggio semplice e chiaro. Descrive la natura della violazione e contiene almeno il nome e i dati di contatto del RPD, le probabili conseguenze, le misure adottate o proposte e, ove utile, le precauzioni che gli interessati possono adottare, come il cambio della password (art. 34, par. 2, GDPR).
- Si effettua con il mezzo **più efficace e diretto**: comunicazione individuale tramite messaggio riservato del registro elettronico, e-mail istituzionale o lettera. La comunicazione deve essere **distinta dalle comunicazioni ordinarie** dell'Istituto e non può essere inserita in avvisi o circolari di contenuto generale. Si redige secondo il modello dell'Allegato E e, per le famiglie che non padroneggiano la lingua italiana, se ne cura ove possibile una versione nella lingua d'origine o un'adeguata mediazione. Non si usano bacheche o comunicazioni collettive che esporrebbero ulteriormente gli interessati.
- La notifica al Garante non sostituisce la comunicazione agli interessati quando questa è evidentemente necessaria, ad esempio se sono stati divulgati online dati sanitari. In circostanze eccezionali e di particolare gravità la comunicazione agli interessati può precedere la notifica al Garante.
- La comunicazione non è dovuta nei casi previsti dall'art. 34, par. 3, GDPR: dati resi incomprensibili, ad esempio mediante cifratura; misure successive che scongiurano il rischio elevato; sforzo sproporzionato, nel qual caso si procede con una comunicazione pubblica di analoga efficacia (ad esempio, un avviso ben visibile sulla home page del sito istituzionale). La ricorrenza dell'esclusione è motivata nella Scheda di valutazione.

9. Fase 6 – Chiusura, misure correttive e Registro

- Conclusa la gestione, e di norma entro 30 giorni, la Dirigente chiude la pratica con una breve **relazione** che documenta i singoli passaggi, le cause accertate e le misure correttive adottate per evitare il ripetersi dell'evento. Tra queste: richiami al personale sugli errori più frequenti, formazione mirata, riesame dei file prima dell'invio, disattivazione tempestiva degli account del personale cessato, modifica delle configurazioni, aggiornamento della DPIA o delle linee guida. La relazione è conservata nel fascicolo riservato della violazione.
- **Ogni violazione, anche non notificata, è annotata nel Registro delle violazioni** (Allegato D), con le circostanze, le conseguenze, i provvedimenti adottati e la motivazione delle decisioni assunte (art. 33, par. 5, GDPR). Vi si annotano anche gli eventi privi di rischio per gli interessati (ad esempio, una breve indisponibilità di una piattaforma o la compromissione di dati già pubblici o cifrati in modo robusto) e i falsi positivi. Il Registro deve essere un elenco dettagliato e consente al Garante di verificare il rispetto dell'art. 33.
- Il Registro e i fascicoli delle singole violazioni sono conservati in forma riservata nella Segreteria Digitale, secondo il Manuale di gestione documentale.

10. Rapporti con i responsabili del trattamento

I fornitori che trattano dati per conto dell'Istituto, in particolare Spaggiari per il registro elettronico e la Segreteria Digitale e Google per Google Workspace for Education, sono tenuti a informare l'Istituto senza ingiustificato ritardo di ogni violazione che li riguardi (art. 33, par. 2, GDPR) e ad assisterlo negli adempimenti (art. 28, par. 3, lett. f, GDPR). Il responsabile non valuta il rischio prima di informare l'Istituto: deve limitarsi ad accertare che si sia verificata una violazione e a comunicarla, perché la valutazione spetta al titolare. Ricevuta una comunicazione del fornitore, la Dirigente avvia la presente Procedura dalla Fase 3. La tempestività della comunicazione del fornitore non sposta il termine di 72 ore, che decorre da quando l'Istituto ne è venuto a conoscenza.

Per gli incidenti che riguardano i **sistemi informativi del Ministero** gestiti a livello centrale (ad esempio SIDI, Anagrafe Nazionale Studenti e relativa partizione separata), compresa la compromissione delle credenziali di accesso del personale, la Dirigente informa senza ritardo lo **CSIRT del Ministero** all'indirizzo CSIRT@istruzione.it, come previsto dalle Linee guida ministeriali per la gestione operativa dei data breach, con copia al RPD. Resta ferma la valutazione degli adempimenti di competenza dell'Istituto per i trattamenti di cui è titolare.

11. Riservatezza e profili disciplinari

Le informazioni sulla violazione sono trattate con riservatezza e comunicate ai soli soggetti che devono intervenire.

La segnalazione tempestiva di un proprio errore è valutata come comportamento collaborativo. Restano ferme le responsabilità per violazioni dolose o gravemente colpose delle istruzioni impartite.

L'omessa o ritardata segnalazione costituisce inosservanza delle disposizioni di servizio. Essa può esporre l'Istituto alle sanzioni amministrative previste dall'art. 83, par. 4, GDPR per la violazione degli obblighi di cui agli artt. 33 e 34.

12. Quadro riepilogativo dei tempi

Momento	Adempimento	Soggetto
Appena si viene a conoscenza dell'evento	Segnalazione interna e prime misure di contenimento	Chiunque rilevi l'evento
Subito dopo la segnalazione	Misure di contenimento ulteriori; coinvolgimento del RPD	Dirigente (o prima collaboratrice); amministratori
Entro 24 ore, ove possibile	Scheda di valutazione e classificazione del rischio	Dirigente con il RPD
Entro 72 ore dalla conoscenza	Notifica al Garante, anche in fasi (se c'è rischio)	Dirigente (o prima collaboratrice)
Senza ingiustificato ritardo	Comunicazione agli interessati (se il rischio è elevato)	Dirigente
Di norma entro 30 giorni	Chiusura, misure correttive, annotazione definitiva nel Registro	Dirigente

13. Riferimenti normativi e documentali

– Regolamento UE 2016/679, artt. 4, n. 12, 24, 28, 32, 33, 34, 39 e 83.

– D.Lgs. 30 giugno 2003, n. 196, come modificato dal D.Lgs. 101/2018, art. 2-quaterdecies.

– EDPB, Linee guida 9/2022 sulla notifica delle violazioni dei dati personali ai sensi del GDPR (versione 2.0 del 28 marzo 2023); Linee guida 01/2021 sugli esempi riguardanti la notifica delle violazioni dei dati personali (14 dicembre 2021).

– Nota MIM – DGPOC, Ufficio III – Protezione dei dati personali, prot. n. 1248 del 28 luglio 2023, “Obblighi di notifica in caso di violazione dei dati personali (c.d. data breach)”, e “Linee guida per la gestione operativa dei data breach” del Ministero (versione agosto 2021).

– Garante per la protezione dei dati personali, provvedimento n. 209 del 27 maggio 2021 (procedura telematica di notifica delle violazioni, operativa dal 1° luglio 2021).

ALLEGATO B

MODULO DI SEGNALAZIONE INTERNA DI VIOLAZIONE DEI DATI PERSONALI

Da inviare immediatamente alla Dirigente Scolastica per e-mail istituzionale con oggetto "URGENTE – SEGNALAZIONE POTENZIALE VIOLAZIONE DATI PERSONALI – RISERVATO". Non allegare i dati o i documenti coinvolti.

1. Chi segnala	
Nome e cognome	
Qualifica / ufficio / plesso	
Recapito telefonico	
2. L'evento	
Data e ora dell'evento (anche presunte)	
Data e ora in cui se ne è venuti a conoscenza	
Che cosa è successo (descrizione sintetica)	
Strumento coinvolto	☐ Registro elettronico ☐ Segreteria Digitale ☐ Gmail ☐ Drive / Classroom ☐ Piattaforma ministeriale ☐ Dispositivo (PC, tablet, smartphone, USB) ☐ Documenti cartacei ☐ Altro: _____
Tipo di evento	☐ Invio o consegna a destinatario errato ☐ Condivisione errata ☐ Accesso non autorizzato / account compromesso ☐ Phishing ☐ Smarrimento o furto ☐ Modifica o cancellazione di dati ☐ Altro
3. I dati coinvolti (per quanto noto)	
Interessati coinvolti	☐ Alunni ☐ Famiglie ☐ Personale ☐ Altri Numero approssimativo: _____
Tipologia di dati	☐ Anagrafici e di contatto ☐ Valutazioni / assenze / note ☐ Dati sanitari, disabilità, DSA, BES ☐ Situazioni familiari o sociali ☐ Credenziali di accesso ☐ Immagini ☐ Altro
Destinatari o soggetti che hanno avuto accesso (se noti)	
4. Prime misure adottate	
Azioni già compiute (es. revoca condivisione, cambio password, richiesta di cancellazione al destinatario)	
Data e firma	

ALLEGATO C

SCHEDA DI VALUTAZIONE DELLA VIOLAZIONE

A. Estremi	
N. progressivo nel Registro	
Data e ora della segnalazione interna	
Data e ora in cui l'Istituto ne è venuto a conoscenza (avvio delle 72 ore)	
Scadenza delle 72 ore	
B. Descrizione	
Tipologia di violazione	☐ Riservatezza ☐ Integrità ☐ Disponibilità
Categorie e numero approssimativo di interessati	
Categorie e volume dei dati	
Presenza di dati particolari o di minori	☐ Sì ☐ No Specificare: _____
Misure di contenimento adottate (con data e ora)	
C. Valutazione del rischio	
Facilità di identificazione degli interessati	☐ Bassa ☐ Media ☐ Alta
Gravità delle possibili conseguenze	☐ Trascurabile ☐ Limitata ☐ Importante ☐ Massima
Probabilità che le conseguenze si verifichino	☐ Trascurabile ☐ Limitata ☐ Importante ☐ Massima
Fattori attenuanti (es. cifratura, cancellazione confermata, revoca senza accessi)	
Esito della valutazione	☐ Rischio improbabile ☐ Rischio ☐ Rischio elevato ☐ Falso positivo (nessuna violazione accertata)
D. Parere del RPD	
Data, modalità e sintesi del parere	
E. Decisione della Dirigente	
Notifica al Garante	☐ Sì – data e ora: _____ n. / ricevuta: _____ ☐ No – motivazione: _____ ☐ Oltre 72 ore – motivi del ritardo: _____
Comunicazione agli interessati	☐ Sì – data, modalità: _____ ☐ No – motivazione (art. 34, par. 3, GDPR): _____
Misure correttive disposte	
Data e firma della Dirigente (o della prima collaboratrice)	

ALLEGATO D

REGISTRO DELLE VIOLAZIONI DEI DATI PERSONALI (art. 33, par. 5, GDPR)

Il Registro è tenuto dalla Dirigente Scolastica in un fascicolo riservato della Segreteria Digitale. Vi si annota ogni violazione, anche se non notificata al Garante.

Per ciascuna violazione si compila una riga dell'indice e si conserva nel fascicolo la relativa Scheda di valutazione (Allegato C).

N.	Data conoscenza	Descrizione sintetica, dati e interessati coinvolti	Esito valutazione	Notifica Garante (data)	Comunicaz. interessati (data)	Chiusura (data)
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						

ALLEGATO E

MODELLO DI COMUNICAZIONE DELLA VIOLAZIONE AGLI INTERESSATI (art. 34 GDPR)

Da inviare individualmente, con il mezzo più diretto (messaggio riservato del registro elettronico, e-mail o lettera), distinta da ogni altra comunicazione. Le parti tra parentesi quadre vanno adattate al caso concreto.

Prot. n. _____ del _____

Alla famiglia dell'alunno/a [nome e cognome] / Al/Alla sig./sig.ra [nome e cognome]

Oggetto: Comunicazione di una violazione dei dati personali che La riguardano – art. 34 del Regolamento UE 2016/679

Gentile [famiglia / sig./sig.ra],

con la presente l'Istituto Comprensivo Statale "Alessandro Volta", titolare del trattamento, La informa di una violazione di sicurezza che ha coinvolto dati personali [Suoi / di Suo/a figlio/a].

Che cosa è accaduto. In data [data] [descrizione semplice e chiara dell'evento, ad esempio: "un documento contenente … è stato inviato per errore a …" / "è stato smarrito …"]. L'Istituto ne è venuto a conoscenza il [data].

Quali dati sono coinvolti. [elenco delle categorie di dati, ad esempio: nome e cognome, classe, valutazioni, informazioni relative a …].

Possibili conseguenze. [descrizione delle conseguenze che potrebbero derivare dalla violazione, ad esempio: conoscenza da parte di terzi di informazioni riservate, tentativi di contatto fraudolento].

Che cosa ha fatto l'Istituto. [misure adottate: ad esempio richiesta di cancellazione al destinatario e relativa conferma, revoca dell'accesso, sospensione dell'account, notifica al Garante per la protezione dei dati personali in data …, misure per evitare che l'evento si ripeta].

Che cosa può fare Lei. [precauzioni consigliate, ad esempio: modificare la password di accesso al registro elettronico; prestare attenzione a messaggi o telefonate sospette che facciano riferimento ai dati coinvolti; segnalarci qualsiasi anomalia].

Per informazioni. Può rivolgersi alla Dirigente Scolastica (miic8eh003@istruzione.it – tel. 02 25492649) o al Responsabile della Protezione dei Dati dell'Istituto, Ing. Antonio Vargiu (dpo@vargiuscuola.it). Resta salvo il diritto di proporre reclamo al Garante per la protezione dei dati personali (www.garanteprivacy.it).

L'Istituto si scusa per l'accaduto e rimane a disposizione per ogni chiarimento.

LA DIRIGENTE SCOLASTICA