ISTITUTO COMPRENSIVO STATALE VALLELUNGA P. - MARIANOPOLI

di Scuola dell'Infanzia, Primaria e Secodaria di 1° grado

Via Agrigento/C.da Piante- Tel. 0934/814079 - Tel. e Fax 0934/814078

e-mail: clic80400g@istruzione.it – sito internet : www.comprensivovallelungavillalba.it

C.A.P. 93010 - Cod. Fisc. 80009750854 – Cod. Mecc. CLIC80400G

ISTITUTO COMPRENSIVO STATALE VALLELUNGA - MARIANOPOLI - -VALLELUNGA PRATAMENO
Prot. 0003964 del 07/07/2023
I-4 (Uscita)

Regolamento in materia di gestione delle violazioni dei dati personali

DATA BREACH

Storia delle modifiche

Versione	Data	Determinazione del Dirigente	Parere del RPD
V.01	15.05.2023	N° 01 del	Positivo, espresso il 13.05.2023 Dott. Alfredo Giangrande

INDICE DEGLI ARGOMENTI

L'Istituzione scolastica
nella persona del Dirigente scolastico

Visti:

- Il Regolamento UE n° 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla protezione dei dati);
- Il d.lgs. n° 196 del 2003 "*Codice in materia di protezione dei dati personali"* e successive modifiche e integrazioni;
- il decreto legislativo n° 51 del 18 maggio 2018;
- Le Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) – WP 250, adottate dal Gruppo di lavoro Art. 29 il 06 febbraio 2018;
- Il Provvedimento n° 157 del Garante del 30 luglio 2019 sulla notifica delle violazioni dei dati personali;
- Le Linee guida in materia di notifica delle violazioni di dati personali (*Examples regarding Data Breach Notification*), adottate dall'*European Data Protection Board* il 14 gennaio 2021;
- Il Provvedimento n° 209 del Garante del 27 maggio 2021 sulla procedura telematica per la notifica di violazioni di dati personali (*data breach*)

EMANA

il seguente Regolamento in materia di gestione
delle violazioni di dati personali

Art. 1
Precisazione sulle premesse

Le premesse che precedono si intendono tutte parte integranti del presente Regolamento.

Art. 2
Premessa

Secondo quanto previsto dall'art. 4 del Regolamento europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, 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*».

È importante riportare, per intero, dispone l'art. 33 del regolamento europeo il cui contenuto ci seguirà lungo la trattazione del tema in questione, rubricato: "*Notifica di una violazione dei dati personali all'autorità di controllo":*

"2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

3. La notifica di cui al paragrafo 1 deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi. 4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo."

In tale contesto, il Regolamento sancisce l'obbligo per il titolare del trattamento di notificare tempestivamente l'avvenuta violazione dei dati personali (c.d. "*Data Breach*") all'autorità di controllo e, in casi determinati e con specifiche modalità, di procedere alla comunicazione direttamente agli interessati.

L'obiettivo delle presenti linee di indirizzo è disciplinare il processo di gestione delle violazioni di dati personali per codesta istituzione scolastica, ossia: definire i principi generali, i ruoli, le responsabilità e le attività da effettuare qualora si verifichi un incidente di sicurezza che comporti la violazione di dati personali.

La presente procedura si applica a tutte le violazioni di dati personali, come di seguito meglio identificate, riscontrate all'interno degli uffici della scuola.

Le disposizioni del presente documento hanno validità per tutti i dipendenti, studenti e genitori, fornitori di beni e servizi, terze parti della scuola.

Art. 3
Definizioni

Di seguito sono riportate le definizioni utili alla comprensione delle presenti linee di indirizzo.

«**Dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

«**Trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

«**Profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

«**Pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

«**Archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

«**Titolare del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

«**Responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

«**Destinatario**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

«**Terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

«**Consenso dell'interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

«**Violazione dei dati personali**»: 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;

«**Dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

«**Dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

«**Dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute. A queste definizioni si affiancano le seguenti, intendendo per:

«**Banca di dati**»: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

«**Evento sulla sicurezza delle informazioni**»: occorrenza identificata di uno stato di un sistema, servizio o rete, che indichi una possibile violazione di una policy sulla sicurezza delle informazioni (Information Security Policy) o il fallimento di controlli, o una situazione precedentemente sconosciuta che può essere rilevante a fini di sicurezza;

«**Incidente sulla sicurezza delle informazioni**»: evento o serie di eventi sulla sicurezza delle informazioni, indesiderati o imprevisti, che hanno una significativa probabilità di compromettere le operazioni aziendali e di minacciare la sicurezza delle informazioni,

Art. 4
Precisazioni sulla definizione di violazione

Per poter porre rimedio a una violazione occorre innanzitutto che il titolare del trattamento sia in grado di riconoscerla. Per far questo, facciamo riferimento alla definizione presentata in premessa.

Seguiamo assieme il percorso raccomandato dal Garante per la protezione dei dati, precisando:

1. **Distruzione**: il significato di "distruzione" dei dati personali sembra essere abbastanza chiaro: si ha distruzione dei dati quando gli stessi non esistono più o non esistono più in una forma che sia di qualche utilità per il titolare del trattamento.
2. **Perdita**: Con "perdita" dei dati personali si deve intendere il caso in cui i dati potrebbero comunque esistere, ma il titolare del trattamento potrebbe averne perso il controllo o l'accesso, oppure non averli più in possesso.
3. **Modifica:** si verifica un danno quando i dati personali sono stati modificati, corrotti o non sono più completi.
4. **Divulgazione o accesso**: un trattamento non autorizzato o illecito può includere la divulgazione di dati personali a (o l'accesso da parte di) destinatari non autorizzati a ricevere (o ad accedere a) i dati oppure qualsiasi altra forma di trattamento in violazione del regolamento.

Ancora, le violazioni possono essere classificate in base ai seguenti tre principi ben noti della sicurezza delle informazioni:

1. "**violazione della riservatezza**", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
2. "**violazione dell'integrità**", in caso di modifica non autorizzata o accidentale dei dati personali;
3. "**violazione della disponibilità**", in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

Va altresì osservato che, a seconda dei casi, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.

Art. 5

Quando è necessario notificare la violazione al Garante o agli interessati.

Quali sono le tempistiche di notifica.

Il regolamento europeo impone al titolare del trattamento di notificare le violazioni all'autorità di controllo competente, fatta salva l'improbabilità che la violazione presenti il rischio che si verifichino detti effetti negativi. Laddove sia altamente probabile che tali effetti negativi si verifichino, lo stesso regolamento impone al titolare del trattamento di comunicare la violazione alle persone fisiche interessate non appena ciò sia ragionevolmente fattibile.

Nel dettaglio l'art. 33, comma 1. del regolamento europeo impone che: "*In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente …omissis. senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone*

fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo."

Il momento esatto in cui il titolare del trattamento può considerarsi "a conoscenza" di una particolare violazione dipenderà dalle circostanze della violazione. In alcuni casi sarà relativamente evidente fin dall'inizio che c'è stata una violazione, mentre in altri potrebbe occorrere del tempo per stabilire se i dati personali sono stati compromessi. Tuttavia, l'accento dovrebbe essere posto sulla tempestività dell'azione per indagare su un incidente per stabilire se i dati personali sono stati effettivamente violati e, in caso affermativo, prendere misure correttive ed effettuare la notifica, ove necessario.

Di conseguenza, il titolare del trattamento dovrebbe disporre di procedure interne per poter rilevare una violazione e porvi rimedio. Ad esempio, per rilevare talune irregolarità nel trattamento dei dati, il titolare o il responsabile del trattamento può utilizzare alcune misure tecniche certe come il flusso di dati e gli analizzatori di registri, dai quali è possibile definire eventi e allerte correlando qualsiasi dato di registro.

È importante che quando viene rilevata una violazione, la stessa venga segnalata al livello superiore appropriato di gestione, in maniera da poter essere trattata e, se del caso, notificata in conformità all'articolo 33 e, se necessario, all'articolo 34 del regolamento europeo.

Art. 6
Procedura da adottare in caso di presunta violazione di dati

Qualora un dipendente dell'amministrazione rilevi una possibile violazione dei dati personali, esso è tenuto ad informarne il Dirigente Scolastico o, qualora esso non sia immediatamente disponibile, il Responsabile della Protezione dei Dati ed altre eventuali figure che gestiscono i sistemi informatici o che forniscono servizi di assistenza e consulenza informatica e normativa in modo da garantire la massima tempestività di intervento.

questo punto il Dirigente scolastico, in concerto con l'RPD e l'amministratore di sistema informatico (qualora si tratti di una violazione informatica), provvederà ad effettuare una prima indagine interna e a definire la gravità dell'eventuale violazione. In particolare, si dovrà procedere a identificare i possibili rischi da essa derivanti e a definire le ulteriori azioni da intraprendere per minimizzare questi rischi.

In questa fase il dirigente scolastico dovrà valutare l'opportunità o la necessità di fare la comunicazione al Garante, che dovrà intervenire entro le 72 ore dalla conoscenza del fatto, ed eventualmente alle persone fisiche minacciate nei loro diritti dall'evento.

In merito alla scelta dovranno essere coinvolti ed esprimeranno il proprio parere il RPD ed eventuali altri consulenti informatico/normativi ma la decisione finale dovrà essere del dirigente scolastico che risponderà di fronte alla legge della scelta operata in base al principio della responsabilizzazione. Nel momento in cui il titolare del trattamento dovesse decidere in modo difforme dal parere del RPD è opportuno che rediga un documento in cui illustri le motivazioni che l'hanno indotto alla scelta.

Qualora il dirigente scolastico ritenesse di dover effettuare la segnalazione al Garante dovrà seguire le istruzioni per l'utilizzo della procedura telematica per la notifica delle violazioni dei dati personali all'indirizzo:

https://servizi.gpdp.it/databreach/s/

Al momento del collegamento apparirà la schermata/menu nella quale sarà possibile prendere le procedure necessarie per effettuare la notificazione delle violazioni al Garante:

In essa sono presenti le rubriche:

- Autovalutazione per la notifica di una violazione dei dati personali
- Compilazione della notifica
- Istruzioni
- informativa sul trattamento dei dati personali
- Pagina informativa – Violazione dei dati personali
- Fac-simile del modello

La violazione, che sia o no comunicata al Garante, dovrà sempre essere annotata nel **registro delle violazioni** che dovrà essere tenuto costantemente aggiornato dalla istituzione scolastica.

Art. 7
Modalità di notifica al Garante a agli interessati

Quando il titolare del trattamento notifica una violazione all'autorità di controllo, l'articolo 33, paragrafo 3 stabilisce che la notifica deve riportare gli elementi elencati in premessa.

l regolamento europeo non definisce le categorie di interessati né le registrazioni di dati personali. Tuttavia, il WP29 suggerisce che le categorie di interessati si riferiscono ai vari tipi di persone fisiche i cui dati personali sono stati oggetto di violazione; pertanto possono essere inclusi includere, tra gli altri, i dati personali di minori e altri gruppi vulnerabili, persone con disabilità, dipendenti o clienti.

In analogia, le categorie di registrazioni di dati personali faranno riferimento anche ai diversi tipi di registrazioni che il titolare del trattamento può trattare, quali dati sanitari, registri didattici, informazioni sull'assistenza sociale, dettagli finanziari, numeri di conti bancari, numeri di passaporto, ecc.

I consideranda 85, 86, 87 e 88 chiariscono e confermano quanto esposto in precedenza e raccomandano di utilizzare tutti i metodi e strategie possibili per mitigare l'accadimento di violazioni di dati personali quali la perdita del controllo di dati personali, il furto o usurpazione d'identità, le perdite finanziarie, la decifratura non autorizzata della pseudonimizzazione, il pregiudizio alla reputazione, la perdita di riservatezza dei dati personali.

Inoltre, Il fatto che non possano non essere disponibili informazioni precise (ad esempio il numero esatto di interessati coinvolti) non dovrebbe costituire un ostacolo alla notifica tempestiva delle violazioni.

Il regolamento consente di effettuare approssimazioni sul numero di persone fisiche interessate e di registrazioni dei dati personali coinvolte. Ci si dovrebbe preoccupare, pertanto, di far fronte agli effetti negativi della violazione piuttosto che di fornire cifre esatte.

Di conseguenza, quando è evidente che c'è stata una violazione ma non se ne conosce ancora la portata, un modo sicuro per soddisfare gli obblighi di notifica è procedere a una notifica per fasi.

Art. 8
Notifica per fasi

Il comma 4. del citato art. 33 del regolamento europeo consente il titolare dei dati di effettuare la notifica per fasi nel caso in cui, al momento dell'evento, non si dispongono di dettagli completi ed esaustivi, quindi il titolare non è nelle condizioni di effettuate la notifica entro le prime 72 ore.

È probabile che ciò si verifichi in caso di violazioni più complesse, quali alcuni tipi di incidenti di sicurezza informatica nel contesto dei quali, ad esempio, può essere necessaria un'indagine approfondita ad opera di esperti, per stabilire in pieno la natura della violazione e la portata della compromissione dei dati personali.

Di conseguenza, in molti casi il titolare del trattamento dovrà effettuare ulteriori indagini e dare seguito alla notifica fornendo informazioni supplementari in un secondo momento. Ciò è consentito a condizione che il titolare del trattamento indichi i motivi del ritardo, ai sensi del comma 1 del citato art. 33.

Il Gruppo di lavoro WP 29 raccomanda che, all'atto della prima notifica all'autorità di controllo, il titolare del trattamento informi quest'ultima del fatto che non dispone ancora di tutte le informazioni richieste e che fornirà ulteriori dettagli in un momento successivo. L'autorità di controllo concorderà le modalità e le tempistiche per la fornitura delle informazioni supplementari. Questo non impedisce al titolare del trattamento di trasmettere ulteriori informazioni in qualsiasi altro momento, qualora venga a conoscenza di ulteriori dettagli rilevanti sulla violazione che devono essere forniti all'autorità di controllo.

L’obiettivo dell’obbligo di notifica consiste nell’incoraggiare il titolare del trattamento ad agire prontamente in caso di violazione, a contenerla e, se possibile, a recuperare i dati personali compromessi e a chiedere un parere pertinente all’autorità di controllo.

La notifica all’autorità di controllo entro le prime 72 ore può consentire al titolare del trattamento di assicurarsi che le decisioni in merito alla notifica o alla mancata notifica alle persone fisiche siano corrette. Tuttavia, lo scopo della notifica all’autorità di controllo non è solo di ottenere orientamenti sull’opportunità di effettuare o meno la notifica alle persone fisiche interessate. In certi casi sarà evidente che, a causa della natura della violazione e della gravità del rischio, il titolare del trattamento dovrà effettuare la notifica alle persone fisiche coinvolte senza indugio.

Ad esempio, se esiste una minaccia immediata di usurpazione d’identità oppure se categorie particolari di dati personali vengono divulgate online, il titolare del trattamento deve agire senza ingiustificato ritardo per contenere la violazione e comunicarla alle persone fisiche coinvolte. In circostanze eccezionali, ciò potrebbe persino aver luogo prima della notifica all’autorità di controllo.

Più in generale, la notifica all’autorità di controllo non può fungere da giustificazione per la mancata comunicazione della violazione all’interessato laddove la comunicazione sia richiesta.

È opportuno, infine, precisare che se, dopo la notifica iniziale, una successiva indagine dimostra che l’incidente di sicurezza è stato contenuto e che non si è verificata alcuna violazione il titolare del trattamento può informarne l’autorità di controllo. Tali informazioni possono quindi essere aggiunte alle informazioni già fornite all’autorità di controllo e l’incidente può essere quindi registrato come un evento che non costituisce una violazione. Non si incorre in alcuna sanzione se si segnala un incidente che alla fine si rivela non essere una violazione.

Art. 9
Notifiche effettuate in ritardo

La normativa in materia chiarisce che, qualora non sia effettuata entro 72 ore, la notifica all'autorità di controllo deve essere corredata dei motivi del ritardo. Questa disposizione, unitamente al concetto di notifica in fasi, riconosce che il titolare del trattamento potrebbe non essere sempre in grado di notificare una violazione entro tale termine e che una notifica tardiva può essere consentita.

Tale ipotesi potrebbe aver luogo, ad esempio, con probabilità limitate, qualora il titolare del trattamento subisca in poco tempo violazioni della riservatezza multiple e simili che coinvolgono allo stesso modo un gran numero di interessati. Il titolare del trattamento potrebbe prendere atto di una violazione e, nel momento in cui inizia l'indagine e prima della notifica, rilevare ulteriori violazioni analoghe, che hanno cause differenti.

A seconda delle circostanze, il titolare del trattamento può impiegare del tempo per stabilire l'entità delle violazioni e, anziché notificare ciascuna violazione separatamente, effettuare una notifica significativa che rappresenta diverse violazioni molto simili tra loro, con possibili cause diverse.

La notifica all'autorità di controllo potrebbe quindi aver luogo in ritardo, oltre le 72 ore previste dopo che il titolare del trattamento sia venuto a conoscenza di tali violazioni.

A rigore di termini, ogni singola violazione costituisce un incidente soggetto a segnalazione. Tuttavia, per evitare che il processo diventi eccessivamente oneroso, il titolare del trattamento può presentare una notifica che cumula tutte le violazioni in questione, a condizione che riguardino il medesimo tipo di dati personali e che questi siano stati violati nel medesimo modo in un lasso di tempo relativamente breve.

Se si verificano diverse violazioni riguardanti tipi diversi di dati personali, violati in maniere diverse, la notifica deve procedere secondo l'iter normale, segnalando ogni violazione ai sensi all'articolo 33.

ebbene il regolamento consenta di effettuare la notifica in ritardo, questa non dovrebbe essere vista come la regola.

È opportuno sottolineare che le notifiche cumulative possono essere effettuate anche per più violazioni analoghe segnalate entro 72 ore.

Art. 10
Notifiche agli interessati

La normativa in materia raccomanda il titolare del trattamento che la notifica all'autorità di controllo è obbligatoria a meno che sia improbabile che dalla violazione possano derivare rischi per i diritti e le libertà delle persone fisiche.

Inoltre, laddove la violazione presenti un rischio elevato per i diritti e le libertà delle persone fisiche occorre informare anche queste ultime. La soglia per la comunicazione delle violazioni alle persone fisiche è quindi più elevata rispetto a quella della notifica alle autorità di controllo, pertanto non tutte le violazioni dovranno essere comunicate agli interessati, il che li protegge da inutili disturbi arrecati dalla notifica.

Il regolamento afferma che la comunicazione di una violazione agli interessati deve avvenire il prima possibile, cioè "senza ingiustificato ritardo".

L'obiettivo principale della comunicazione agli interessati consiste nel fornire loro informazioni specifiche sulle misure che questi possono prendere per proteggersi. Come osservato in precedenza, a seconda della natura della violazione e del rischio presentato, la comunicazione tempestiva aiuterà le persone a prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione.

Art. 11
Informazioni da fornire agli interessati

Il titolare comunicherà all'interessato la natura della violazione dei suoi dati personali utilizzando un linguaggio semplice e chiaro, fornendo alcune informazioni quali:

- una descrizione della natura della violazione;
- il nome e i dati di contatto del responsabile della protezione dei dati;
- una descrizione delle probabili conseguenze della violazione;
- una descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi;
- fornire suggerimenti sul modo in cui proteggersi dalle possibili conseguenze negative della violazione, come modificare le password in caso di compromissione delle credenziali di accesso.

Il titolare comunicherà direttamente agli interessati coinvolti utilizzando i mezzi di comunicazione più accessibili, veloci, idonei e che massimizzi la possibilità di fornire informazioni correttamente a tutte le persone interessate.

Il titolare del trattamento potrebbe utilizzare diversi metodi di comunicazione, anziché un singolo canale di a seconda delle circostanze.

Art. 12
Casi nei quali non è richiesta la comunicazione agli interessati

L'articolo 34 comma 3 del regolamento europeo, stabilisce tre condizioni che, se soddisfatte, non richiedono la comunicazione agli interessati in caso di violazione, ossia:

1. il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
2. il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
3. detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Nel caso in cui il titolare del trattamento abbia deciso di non comunicare la violazione di dati personali agli interessati, deve far menzione all'interno del registro delle violazioni delle ragioni a fondamento della propria decisione. In tal caso, l'Autorità di controllo, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato per i diritti e le libertà degli interessati, può chiedere al titolare che provveda alla comunicazione ovvero può ritenere che una delle condizioni più sopra menzionate sia soddisfatta.

Art. 13
Procedura di risposta ad una violazione di dati

Questa istituzione scolastica risponderà di qualsiasi sospetta o presunta violazione dei dati.

La scuola deve essere preparata a rispondere a qualunque violazione sempre per tutti gli anni scolastici.

Le violazioni sono gestite dal titolare del trattamento, in persona del dirigente scolastico, sotto la supervisione del responsabile della protezione dei dati.

Pertanto, tutti gli operatori scolastici che quotidianamente, in ragione del loro lavoro, trattano dati personali, saranno informati e formati adeguatamente attraverso corsi d'istruzione a cui saranno chiamati a partecipare obbligatoriamente.

Il dirigente sarà immediatamente informato della sospetta o presunta violazione riscontrata e, dopo una prima sommaria valutazione deciderà se:

1. si tratta di un incidente ritenuto "falso positivo" che cioè indica un risultato positivo o anormale quando, di fatto è effettivamente presente, una condizione normale. In questo caso la procedura sarà chiusa.
2. altrimenti, sentito il parere del responsabile della protezione dei dati, si tratta di una violazione accertata.

In questo secondo caso il dirigente avvierà un'indagine corretta ed imparziale, che porterà alla valutazione del rischio che presenterà una delle seguenti possibilità:

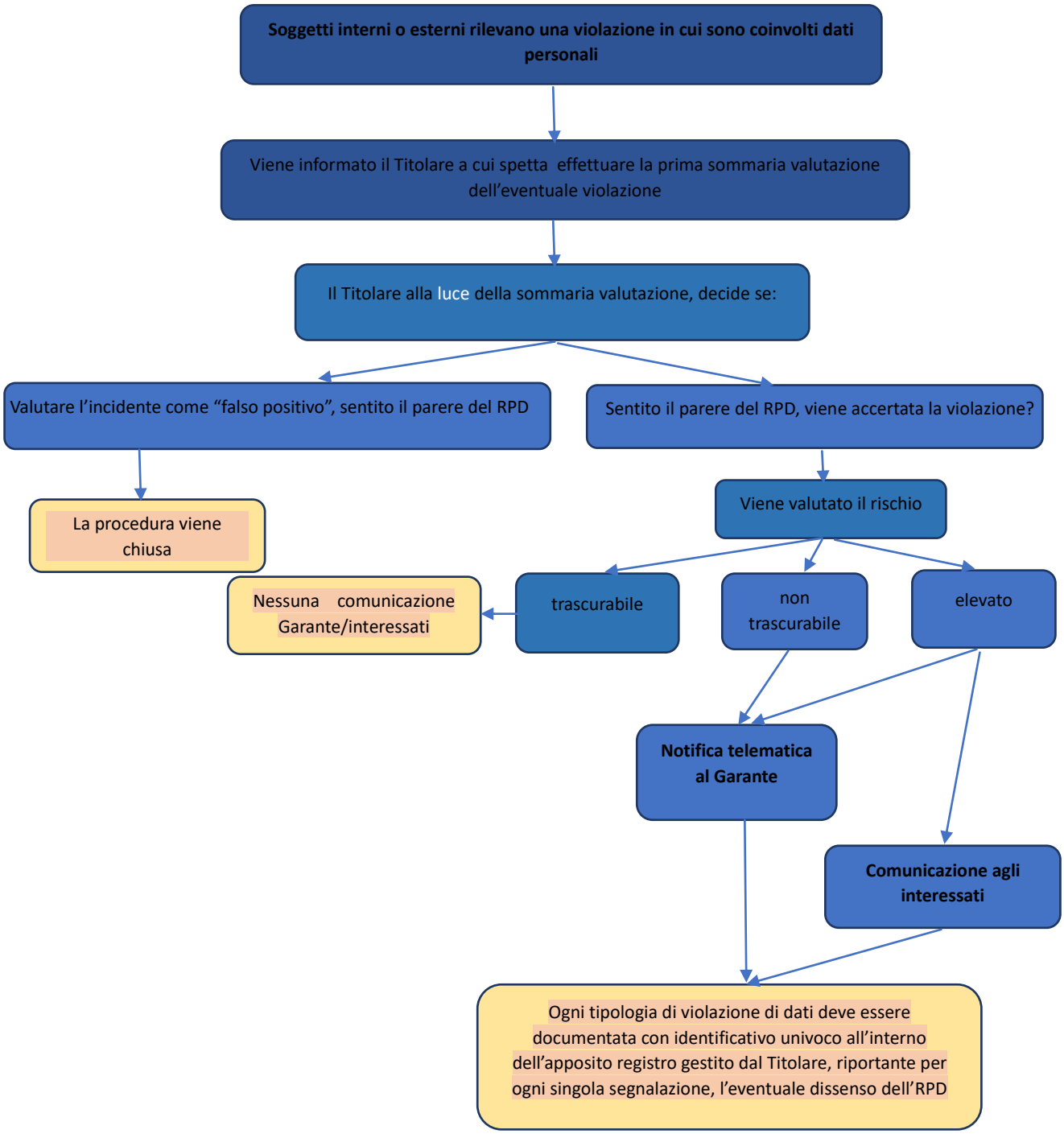
1. rischio **trascurabile**: il dirigente non effettuerà alcuna comunicazione al Garante e agli interessati.
2. rischio **non trascurabile** od **elevato**: il dirigente notificherà telematicamente al Garante l'avvenuta violazione e darà notizia agli interessati dell'incidente.

Il dirigente ultimerà la procedura identificando i requisiti per la risoluzione e monitorando la soluzione, coordinandosi, infine, con le autorità competenti, ove necessario.

Completate le procedure, il dirigente aggiornerà, senza alcun indugio, il registro delle violazioni.

Art. 14
Schema delle procedure di valutazione delle violazioni di dati personali

Il presente schema visualizza, in maniera schematica e più leggibile, quanto espresso testualmente nell'articolo che precede.



Art. 15
Scheda dell'evento

Esempio di scheda al cui interno sono contenuti i seguenti dati:

SCHEDA EVENTO	
Codice evento	DB_01
Data e ora della violazione anche solo se presunta, specificando se è presunta	
Data ed ora in cui si è avuta conoscenza della violazione	
Fonte della segnalazione	
Tipologia dell'evento anomalo	
Descrizione dell'evento anomalo	
Numero di interessati coinvolti	
Numerosità di dati personali di cui si presume la violazione	
Luogo in cui è avvenuta la violazione dei dati: specificare se è avvenuta a seguito di smarrimento di dispositivi o di supporti portatili	
Descrizione dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti, con indicazione della loro ubicazione	

Art. 16
Classificazione degli eventi

A) La classificazione degli eventi risponde ai seguenti possibili casi, suscettibili di aggiornamenti:

1. Divulgazione di dati a persone non autorizzate;
2. Perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
3. Perdita o furto di documenti cartacei;
4. Illecito da parte di un dipendente [ad es.: violazione causata da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia che distribuisce in ambiente pubblico];
5. Accesso abusivo [ad es.: violazione causata da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite];
6. Casi di pirateria informatica;
7. Banche dati alterate o distrutte senza autorizzazione rilasciata dal Dirigente scolastico;
8. Virus o altri attacchi al sistema informatico o alla rete della scuola;
9. Violazione di misure di sicurezza fisica [ad es.: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate];
10. Smarrimento di pc portatili, dispositivi o attrezzature informatiche scolastiche;
11. Invio di email contenenti dati personali e/o particolari a erroneo destinatario.

B) Il rischio di una valutazione di violazione di dati personali, viene valutato secondo i seguenti livelli:

- rischio **trascurabile;**
- rischio **non trascurabile**;
- rischio **elevato**.

I risultati ottenuti dalla valutazione del rischio verranno sinteticamente riportati nello schema che segue:

Scheda violazione dati		
Codice evento	Classificazione evento	Rischio evento
DB_01		

Art. 17
Registro delle violazioni

Il registro delle violazioni di dati personali deve essere continuamente aggiornato in funzione del verificarsi di eventi in cui si ritiene che siano coinvolti dati personali.

Il Dirigente scolastico deve documentare qualsiasi violazione di dati personali, anche quelle che non comportano l'obblio di comunicazione al Garante o agli interessati.

Esso può essere gestito in modalità cartacea ed anche in quella informatica e pubblicato in Amministrazione Trasparente rispettando le regole prescritte per tale pubblicazione.

Evento				Conseguenze	Provvedimenti adottati	Notifica alla autorità di controllo		Comunicazione allo interessato	
Codice evento	Trascurabile	Non trascurabile	Elevato			Si/No	Data	Si/No	Data

LOREDANA
PAOLA
MATRAXIA
07.07.2023
11:30:28
GMT+01:00