



ISTITUTO GLOBALE SANT'ANTIOCO
Via Virgilio, 17 - SANT'ANTIOCO (CA) 09017 ☎ 0781- 83095 📠 0781-802046 📠
Codice meccanografico ministeriale CAIC87700N -Codice fiscale 90027650929
Indirizzo di posta elettronica caic87700n@istruzione.it -
Indirizzo di posta elettronica certificata caic87700n@pec.istruzione.it
Sito web www.icsantantiococalasetta.edu.it

*Agli alunni
Ai genitori/tutori degli alunni
Al personale docente e ATA
Ai prestatori d'opera e ai collaboratori
All'Albo
Amministrazione trasparente*

OGGETTO: Pubblicazione “Disposizioni organizzative per la gestione delle violazioni dei dati personali”

Si porta all'attenzione dell'utenza e di tutto il personale impiegato a vario titolo nell'Istituto delle Disposizioni organizzative per la gestione delle violazioni dei dati personali di cui al documento allegato alla cui attenta lettura si rinvia e che ciascun soggetto in indirizzo è tenuto ad osservare per quanto di propria competenza. **In data odierna e per 15 giorni consecutivi il documento viene pubblicato all'albo dell'Istituto con valore di notifica agli interessati.**

Il Regolamento Generale sulla Protezione dei Dati (Reg. UE 679/2016), di seguito il Regolamento, introduce l'obbligo di notificare una violazione dei dati personali (in appresso: “violazione”) all'autorità di controllo nazionale competente (oppure, in caso di violazione transfrontaliera, all'autorità capofila) e, in alcuni casi, di comunicare la violazione alle singole persone fisiche i cui dati personali sono stati interessati dalla violazione.

Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il Titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

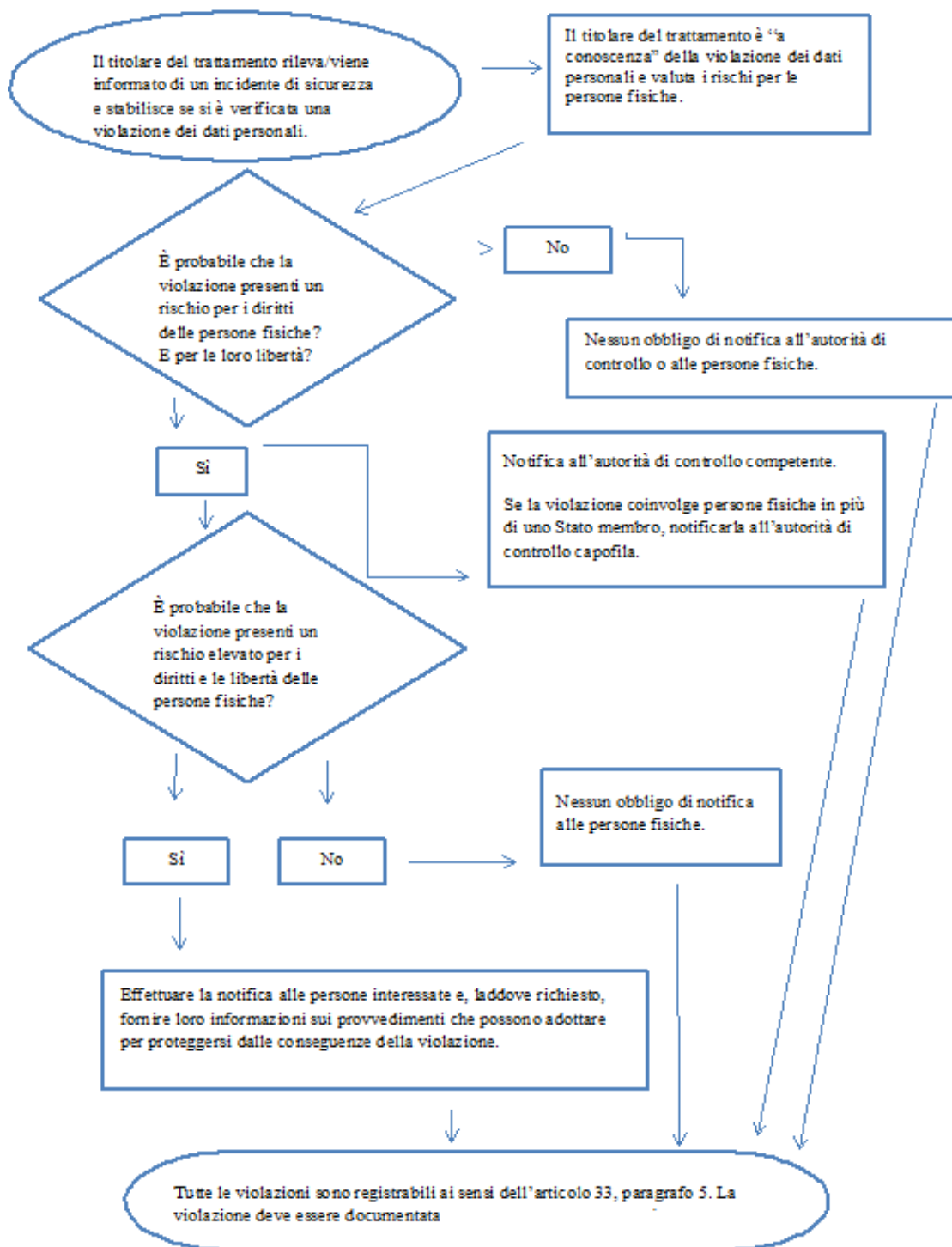
Al fine di identificare e, se necessario, notificare correttamente un data breach all'autorità garante competente e/o agli interessati, il Dirigente Scolastico intende definire le procedure da seguire qualora avvenga un presunto data breach all'interno dell'amministrazione. Si ricorda che la mancata notifica, qualora sia essa necessaria, può comportare una sanzione amministrativa fino ad un importo di 10 milioni di euro o, nel caso di società, al 2% del fatturato dell'intera società.

Il documento contenente le disposizioni organizzative per la gestione delle violazioni dei dati personali è stato redatto sulla base delle Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679, redatto dal gruppo di lavoro articolo 29 per la protezione dei dati, adottate il 3 ottobre 2017 e nella versione emendata e adottata in data 6 febbraio 2018. Tali linee guida sono reperibili sul sito del garante per la protezione dei dati personali al link <https://www.garanteprivacy.it/regolamentoue/databreach>.

ALLEGATI

Vengono di seguito riportate le istruzioni schematiche relative alla notifica della violazione (allegato A), ed una lista non esaustiva delle possibili violazioni (allegato B), come indicato dall'autorità Garante per la Protezione dei Dati Personali.

Allegato A: schematizzazione delle procedure di valutazione delle violazioni di dati personali



Allegato B: Esempi di violazioni dei dati personali e dei soggetti a cui notificarle

I seguenti esempi non esaustivi aiuteranno il titolare del trattamento a stabilire se deve effettuare la notifica in diversi scenari di violazione dei dati personali. Questi esempi possono altresì contribuire a distinguere tra rischio e rischio elevato per i diritti e le libertà delle persone fisiche.

Esempio	Notifica all'autorità di controllo?	Comunicazione all'interessato?	Note/raccomandazioni
Un titolare del trattamento ha effettuato un backup di un archivio di dati personali crittografati su una chiave USB. La chiave viene rubata durante un'effrazione.	No.	No.	Fintantoché i dati sono crittografati con un algoritmo all'avanguardia, esistono backup dei dati, la chiave univoca non viene compromessa e i dati possono essere ripristinati in tempo utile, potrebbe non trattarsi di una violazione da segnalare. Tuttavia, se la chiave viene successivamente compromessa, è necessaria la notifica.
ii. Un titolare del trattamento gestisce un servizio online. A seguito di un attacco informatico ai danni di tale servizio, i dati personali di persone fisiche vengono prelevati. Il titolare del trattamento ha clienti in un solo Stato membro.	Sì, segnalare l'evento all'autorità di controllo se vi sono probabili conseguenze per le persone fisiche.	Sì, segnalare l'evento alle persone fisiche a seconda della natura dei dati personali interessati e se la gravità delle probabili conseguenze per tali persone è elevata.	
iii. Una breve interruzione di corrente di alcuni minuti presso il call center di un titolare del trattamento impedisce ai clienti di chiamare il titolare del trattamento e accedere alle proprie registrazioni.	No.	No.	Questa non è una violazione soggetta a notifica, ma costituisce comunque un incidente registrabile ai sensi dell'articolo 33, paragrafo 5. Il titolare del trattamento deve conservare adeguate registrazioni in merito.
iv. Un titolare del trattamento subisce un	Sì, effettuare la segnalazione	Sì, effettuare la segnalazione alle	Se fosse stato disponibile un backup e i dati

<p>attacco tramite <i>ransomware</i> che provoca la cifratura di tutti i dati. Non sono disponibili backup e i dati non possono essere ripristinati. Durante le indagini, diventa evidente che l'unica funzionalità dal <i>ransomware</i> era la cifratura dei dati e che non vi erano altri <i>malware</i> presenti nel sistema.</p>	<p>all'autorità di controllo, se vi sono probabili conseguenze per le persone fisiche in quanto si tratta di una perdita di disponibilità.</p>	<p>persone fisiche, a seconda della natura dei dati personali interessati e del possibile effetto della mancanza di disponibilità dei dati, nonché di altre possibili conseguenze.</p>	<p>avessero potuto essere ripristinati in tempo utile non sarebbe stato necessario segnalare la violazione all'autorità di controllo o alle persone fisiche, in quanto non si sarebbe verificata nessuna perdita permanente di disponibilità o di riservatezza. Tuttavia, qualora l'autorità di controllo fosse venuta a conoscenza dell'incidente con altri mezzi, avrebbe potuto prendere in considerazione lo svolgimento di un'indagine al fine di valutare il rispetto dei requisiti di sicurezza più ampi di cui all'articolo 32.</p>
<p>v. Una persona telefona al call center di una banca per segnalare una violazione dei dati. La persona ha ricevuto l'estratto conto mensile da un soggetto diverso.</p> <p>Il titolare del trattamento intraprende una breve indagine (ossia la conclude entro 24 ore) e stabilisce con ragionevole certezza che si è verificata una violazione dei dati personali e che vi è una potenziale carenza sistemica che potrebbe comportare il coinvolgimento già occorso o potenziale di altre persone fisiche.</p>	<p>Sì.</p>	<p>La comunicazione va effettuata soltanto alle persone fisiche coinvolte in caso di rischio elevato e se è evidente che altre persone fisiche non sono state interessate dall'evento.</p>	<p>Se dopo ulteriori indagini si stabilisce che l'evento ha interessato un numero maggiore di persone fisiche è necessario comunicare questo sviluppo all'autorità di controllo, e il titolare del trattamento deve informarne le altre persone fisiche interessate se sussiste un rischio elevato per loro.</p>

vi. Un titolare del trattamento gestisce un mercato online e ha clienti in più Stati membri. Tale mercato subisce un attacco informatico a seguito del quale i nomi utente, le password e la cronologia degli acquisti vengono pubblicati online dall'autore dell'attacco.	Sì, segnalare l'evento all'autorità di controllo capofila se la violazione riguarda un trattamento transfrontaliero.	Sì, dato che la violazione potrebbe comportare un rischio elevato.	<p>Il titolare del trattamento dovrebbe prendere delle misure, ad esempio forzare il ripristino delle password degli account interessati, e altri provvedimenti per attenuare il rischio.</p> <p>Il titolare del trattamento dovrebbe altresì considerare qualsiasi altro obbligo di notifica, ad esempio ai sensi della direttiva NIS, trattandosi di un fornitore di servizi digitali.</p>
vii. Una società di <i>hosting</i> di siti web che funge da responsabile del trattamento individua un errore nel codice che controlla l'autorizzazione dell'utente. A causa di tale vizio, qualsiasi utente può accedere ai dettagli dell'account di qualsiasi altro utente.	<p>In veste di responsabile del trattamento, la società di <i>hosting</i> di siti web deve effettuare la notifica ai clienti interessati (i titolari del trattamento) senza ingiustificato ritardo.</p> <p>Supponendo che la società di <i>hosting</i> di siti web abbia condotto le proprie indagini, i titolari del trattamento interessati dovrebbero essere ragionevolmente certi di aver subito una violazione e pertanto è probabile che vengano considerati "a conoscenza" della violazione nel momento in cui hanno ricevuto la notifica da parte della società di <i>hosting</i> (il responsabile del trattamento). Il titolare del trattamento deve quindi effettuare la notifica all'autorità di controllo.</p>	Qualora non vi siano probabili rischi elevati per le persone fisiche non è necessario effettuare una comunicazione a tali persone.	<p>La società di <i>hosting</i> di siti web (responsabile del trattamento) deve prendere in considerazione qualsiasi altro obbligo di notifica (ad esempio ai sensi della direttiva NIS, trattandosi di un fornitore di servizi digitali).</p> <p>Qualora non vi sia alcuna prova che tale vulnerabilità sia sfruttata presso uno dei suoi titolari del trattamento, la violazione potrebbe non essere soggetta all'obbligo di notifica, tuttavia potrebbe essere una violazione da registrare o essere il segno di un mancato rispetto dell'articolo 32.</p>

viii. Le cartelle cliniche di un ospedale sono indisponibili per un periodo di 30 ore a causa di un attacco informatico.	Sì, l'ospedale è tenuto a effettuare la notifica in quanto può verificarsi un rischio elevato per la salute e la tutela della vita privata dei pazienti.	Sì, informare le persone fisiche coinvolte.	
ix. I dati personali di un gran numero di studenti vengono inviati per errore a una mailing list sbagliata con più di 1 000 destinatari.	Sì, segnalare l'evento all'autorità di controllo.	Sì, segnalare l'evento alle persone fisiche coinvolte in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.	
x. Una e-mail di marketing diretto viene inviata ai destinatari nei campi "a:" o "cc:", consentendo così a ciascun destinatario di vedere l'indirizzo e-mail di altri destinatari.	Sì, la notifica all'autorità di controllo può essere obbligatoria se è interessato un numero elevato di persone, se vengono rivelati dati sensibili (ad esempio una mailing list di uno psicoterapeuta) o se altri fattori presentano rischi elevati (ad esempio, il messaggio di posta elettronica contiene le password iniziali).	Sì, segnalare l'evento alle persone fisiche coinvolte in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.	La notifica potrebbe non essere necessaria se non vengono rivelati dati sensibili e se viene rivelato soltanto un numero limitato di indirizzi di posta elettronica.

Il Dirigente Scolastico
Tiziana Meloni

Firma autografa omessa ai sensi dell'art. 3 del D. Lgs n. 39/1993