ISTITUTO COMPRENSIVO DI MAJANO e FORGARIA
SCUOLE DELL'INFANZIA, PRIMARIA E SECONDARIA DI 1° GRADO
Comuni di Majano e Forgaria nel Friuli
Viale G. Schiratti,1 - 33030 MAJANO (UD)
tel. 0432959020 - fax 0432948208 - C.F. 80015380308
web: www.majanoscuole.it - *e-mail:* udic81500t@istruzione.it
pec: udic81500t@pec.istruzione.it

Prot. n.

Majano, 21 maggio 2021

Alla DSGA dell'IC Majano e Forgaria
Agli AA dell'IC Majano e Forgaria

OGGETTO: POLICY PER LA GESTIONE DEL DATA BREACH

Istituto Comprensivo Majano e Forgaria

Rev.	Date	Description	Emesso	Controllato	Approvato
DB.R1	21/10/2020	Stesura policy per la gestione del data breach	CORSINI	D.S.	D.S.

Le variazioni della revisione sono evidenziate in rosso.

POLICY PER LA GESTIONE DEL DATA BREACH

Premessa

1) Definizione di Data Breach (violazione di dati personali)
2) Individuazione di un Data Breach
3) Individuazione dei soggetti interni preposti alla gestione del Data Breach
4) Comunicazione della violazione al soggetto preposto alla gestione del Data Breach
5) Individuazione delle modalità con le quali il responsabile deve comunicare al titolare del trattamento la sua violazione di dati
6) Definizione dei tempi di notifica del Data Breach

Procedura

7) Analisi del Data Breach
8) Tipo di dati coinvolti
9) Verifica della gravità e del possibile impatto sui dati

10) Compilazione del registro delle violazioni
11) Decidere se fare la notifica all'Autorità Garante e agli interessati
12) Definizione del contenuto della notifica
13) Casi da non notificare all'Autorità Garante
14) Processo di verifica della policy

PREMESSA

1) Definizione di Data Breach (violazione di dati personali)

Per data Breach si intende una 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, par.12 GDPR).
Distruzione: situazione nella quale il dato non esiste più o non esiste più in una forma che possa essere utilizzato dal titolare del trattamento.
Modifica: situazione nella quale il dato personale è stato alterato, corrotto o non è più completo
Perdita: situazione nella quale il dato personale esistere ancora, ma il titolare del trattamento ha perso il controllo sullo stesso, l'accesso al dato o il dato non è più in suo possesso.
Divulgazione non autorizzata / illegale: situazione nella quale il dato è stato divulgato a destinatari che non erano autorizzati a riceverlo o ad averne accesso, qualunque altro trattamento in violazione del GDPR.

2) Individuazione di un Data Breach

Di seguito si indicano alcuni esempi, senza pretesa di esaustività, di Data Breach al fine di aiutare i dipendenti a riconoscere le situazioni che necessitano di essere prontamente segnalate:

- accesso da parte di terzi non autorizzati (ad esempio, un attacco ransomware che comporta la crittografia dei dati e non è disponibile un backup degli stessi);
- azione deliberata o accidentale (o inerzia) da parte del Titolare o del Responsabile;
- invio di dati personali a un destinatario errato;
- dispositivi informatici (esempio notebook, chiavette usb, cd/dvd,..) contenenti dati personali (non crittografati) persi o rubati;
- alterazione dei dati personali senza permesso;
- perdita di disponibilità di dati personali (es. situazione nella quale l'unica copia di una parte di dati personali è stata crittografata da un ramsonware o dal titolare del trattamento utilizzando una chiave che non è più in suo possesso; cancellazione accidentale o non autorizzata di dati personali; quando il titolare non può fare un restore dei dati dal backup, significativa interruzione delle normali attività Istituzionali, ad esempio, a seguito di blackout elettrico, attacco di *denial of service* che rendano indisponibili i dati personali)

Non è da intendersi violazione di sicurezza un'azione di manutenzione pianificata al sistema informativo in quanto non rientra nella definizione data dall'art. 4, par. 12 GDPR.

3) Individuazione dei soggetti interni preposti alla gestione del Data Breach

In caso di perdita o distruzione, anche accidentali, di dati personali (quindi anche dei documenti cartacei o informatici e/o dei supporti che li contengono), e in generale in tutti i casi in cui l'Incaricato ritenga ragionevolmente che vi possa essere stata una violazione degli stessi (distruzione o perdita - anche accidentali, accessi indebiti, non autorizzati, modifica non autorizzata, furto/perdita/sottrazione di password, divulgazione non autorizzata di dati personali, ecc.), il dipendente che ne viene a conoscenza è tenuto a darne comunicazione immediata al DIRIGENTE SCOLASTICO quale preposto alla gestione della violazione e, per opportuna conoscenza, al Responsabile della protezione dei dati Avv. Stefano Corsini (**dpo@avvocatocorsini.it**).

4) Comunicazione della violazione al soggetto preposto alla gestione del Data Breach

La violazione di dati personali va comunicata al Dirigente Scolastico sia verbalmente sia tramite email al seguente indirizzo istituzionale ***udic81500t@istruzione.it***.

5) Individuazione delle modalità con le quali il dipendente e il Responsabile devono comunicare al titolare del trattamento la violazione di dati

Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione (Art. 33 par. 2). Allo stesso modo deve procedere il dipendente della Scuola. I responsabili del trattamento e i dipendenti incaricati che a vario titolo trattano i dati per conto della scuola devono comunicare la violazione di sicurezza eventualmente subita all'interno della loro struttura senza ingiustificato ritardo dalla presa di coscienza della stessa. L'Istituto ha stabilito che tale comunicazione va indirizzata al seguente indirizzo email: *udic81500t@istruzione.it*. I dipendenti con diritto di accesso a questa casella di posta sono tenuti ad allertare immediatamente il Dirigente Scolastico e, per opportuna conoscenza, il Responsabile della protezione dei dati nel momento stesso in cui si riceva una comunicazione inerente una violazione di dati personali da parte di un dipendente o collaboratore della Scuola o da un responsabile esterno.

6) Definizione dei tempi di notifica del Data Breach (art. 33, par. 1 GDPR)

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione 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 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.

PROCEDURA

7) Analisi del Data Breach

La violazione di sicurezza dei dati personali può essere di tre tipi, in particolare può riguardare:
- perdita di confidenzialità: si verifica quando c'è una divulgazione non autorizzata o accidentale di dati personali o un accesso agli stessi
- perdita di integrità: si verifica quando il dato personale viene modificato in modo accidentale o non autorizzato.
- perdita di disponibilità (definita come "garantire l'accesso e l'uso tempestivo e affidabile delle informazioni"): si verifica quando c'è un perdita di accesso ai dati accidentale o non autorizzata o la distruzione degli stessi.

E' necessario identificare subito a quale di queste tipologie appartiene la violazione subita dall'Istituto.

8) Tipo di dati coinvolti

I dati personali che possono essere coinvolti in una violazione sono di tre tipi:
- Dati personali: 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 (art. 4 par.1 GDPR)
- Categorie particolari di dati: dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona
- Dati relativi a condanne penali e reati

E' necessario identificare quale tra queste tipologie di dati sono coinvolti nella violazione di sicurezza.

9) Verifica della gravità e del possibile impatto sui dati personali

Nella valutazione, il Titolare del trattamento deve tenere conto della probabilità del rischio e della sua gravità basandosi su:

- Caratteristiche peculiari degli Interessati: alcune categorie di soggetti, ad esempio i bambini, rischiano di essere maggiormente esposti in caso di violazione.
- Numero di individui Interessati: maggiore è il numero di soggetti, maggiori rischiano di essere le implicazioni di un'eventuale Data Breach. Anche in questo caso, però, è necessario valutare le circostanze, in quanto, in alcuni casi, la violazione può comportare gravi rischi anche per il singolo.
- Eventuali caratteristiche del Titolare del trattamento: anche questo è un elemento da tenere in considerazione, infatti, a seconda del tipo di attività svolta, la violazione può essere più o meno grave.

E' necessario che i preposti alla gestione del Data Breach effettuino una verifica della gravità della violazione di sicurezza e delle possibili conseguenze che la stessa può avere sui diritti e le libertà fondamentali delle persone fisiche coinvolte.

10) Compilazione del registro delle violazioni

Il Titolare del trattamento deve documentare 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 di quanto previsto dalla normativa (art. 33 par 5 GDPR).

I preposti alla gestione del Data Breach devono raccogliere dai loro colleghi tutte le informazioni utili ed annotare di conseguenza, senza ingiustificato ritardo, nel registro delle violazioni tutte le violazioni di sicurezza che coinvolgono dati personali.

Vanno documentate nel registro anche le violazioni che implicano una perdita temporanea di disponibilità dei dati (es. mancanza di corrente elettrica per un breve lasso di tempo).

11) Decidere se fare la notifica all'Autorità Garante e agli interessati

Quando una violazione di sicurezza comporta un rischio elevato per i diritti e le libertà degli interessati è necessario fare la notifica all'Autorità Garante.

Di seguito si indicano alcuni esempi, senza pretesa di esaustività, che richiedono la notifica all'Autorità Garante in modo da facilitare i preposti alla gestione del Data Breach nelle decisioni da adottare in questa situazione.

- Il furto di un database di clienti, i cui dati possono essere utilizzati per commettere frodi attraverso le identità sottratte, deve essere notificato, dato l'impatto che questo potrebbe avere su quegli individui che potrebbero subire perdite finanziarie o altre conseguenze.
- Perdita di controllo sui dati personali
- limitazione dei diritti degli interessati, loro discriminazione o possibile danno reputazionale
- Perdita di confidenzialità di dati personali protetti da segreto professionale
- Svantaggio economico sociale per gli interessati
- mancanza di backup dei dati personali oggetto della violazione di sicurezza, anche se crittografati

12) Definizione del contenuto della notifica

La notifica di una violazione all'Autorità di controllo deve almeno (art. 33 par. 3):

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.

Per la comunicazione è preferibile utilizzare il modello predisposto dal Garante con il Provvedimento n. 157 del 30/7/2019 allegato alla presente.

Comunicazione di una violazione di dati personali all'interessato (art. 34 GDPR)

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

La comunicazione all'interessato descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di seguito indicate:

- il nome e i dati di contatto del Responsabile della Protezione dei Dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrizione delle probabili conseguenze della violazione dei dati personali
- descrizione delle 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

Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

a. 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
b. 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
c. 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 non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni è soddisfatta.

13) Casi da non notificare all'Autorità Garante

Quando la violazione di sicurezza non comporta un rischio elevato per i diritti e le libertà degli interessati la notifica all'Autorità Garante non è richiesta.

Di seguito si forniscono alcuni esempi, senza pretesa di esaustività, di casi che non necessitano la notifica all'Autorità Garante al fine di aiutare i preposti alla gestione del Data Breach nelle decisioni che si troveranno a prendere nell'affrontare questa situazione.

- la perdita o l'alterazione inappropriata di una rubrica del personale
- la predita di disponibilità di dati personali che erano crittografati con un algoritmo allo stato dell'arte, dei quali esiste un backup per il ripristino degli stessi in tempi brevi e la cui chiave di decriptazione non è stata compromessa.
- mancanza di corrente per un lasso di tempo breve che rende indisponibile i dati personali

14) Processo di verifica della policy

La presente policy sarà verificata dal titolare del trattamento con cadenza annuale per verificare la sua rispondenza alle esigenze e alle eventuali nuove situazioni che potrebbero verificarsi in Istituto.

IL DIRIGENTE SCOLASTICO
Francesco Candido

Firma autografa sostituita a mezzo stampa digitale ai sensi dell'art. 3/D.to Lgs 12.02.1993, n. 39