Data Breach Policy

Procedura di notifica di violazione dei dati personali

INDICE

Sommario

PREMESSA 3
SCOPO 3
COS'E UNA VIOLAZIONE DEI DATI PERSONALI (DATABREACH) 4
A CHI SONO RIVOLTE QUESTE PROCEDURE? 4
A QUALI TIPI DI DATI SI RIFEREISCE QUESTA PROCEDURA 5
GESTIONE COMUNICAZIONE DI DATABREACHES 5
GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI 5
Step 1: Identificazione e indagine preliminare 5
Step 2: Contenimento, Recovery e risk assessment 6
Step 3: Notifica all'Autorità Garante competente (eventuale) 6
Step 4: Comunicazione agli interessati (eventuale) 6
Step 5: Documentazione della violazione 7
ALLEGATO A – MODULO DI COMUNICAZIONE DATA BREACH 8
ALLEGATO B – MODULO DI VALUTAZIONE DEL RISCHIO CONNESSO ALDATA BREACH 9

PREMESSA

L' Istituto Comprensivo Grosseto 6, ai sensi del Regolamento Europeo 2016/679 (da qui in avanti GDPR), è tenuta a mantenere sicuri i dati personali trattati nell'ambito delle proprie attività istituzionali e ad agire senza ingiustificato ritardo in caso di violazione dei dati stessi (incluse eventuali notifiche all'Autorità Garante competente ed eventuali comunicazioni agli interessati).
È di fondamentale importanza predisporre azioni da attuare nell'eventualità in cui si presentino violazioni concrete, potenziali o sospette di dati personali, ciò al fine di evitare rischi per i diritti e le libertà degli interessati, nonché danni economici all'Istituto, e per poter comunicare nei tempi e nei modi previsti dalla normativa europea all'Autorità Garante e/o agli interessati.
Le sanzioni previste dal GDPR per omessa notifica di Data Breach all'Autorità di Controllo o omessa comunicazione agli interessati o entrambi gli adempimenti, nei casi in cui siano soddisfatti i requisiti di cui agli artt. 33 e 34 GDPR, può comportare l'applicazione in capo all'ENTE di una sanzione amministrativa pecuniaria fino a 10 milioni di euro o fino al 2% del "fatturato" annuo totale dell'esercizio precedente, anche accompagnata da una misura correttiva ai sensi dell'art. 58 c. 2.

SCOPO

Lo scopo di questa procedura è di disegnare un flusso per la gestione delle violazioni di dati personali trattati dall'Istituto Comprensivo Grosseto 6 inqualità di Titolare del trattamento (di seguito "Titolare del trattamento").

COS'E UNA VIOLAZIONE DEI DATI PERSONALI (DATABREACH)

Una violazione di dati personali è ogni infrazione alla sicurezza degli stessi che comporti - 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 dal Titolare del trattamento.

Le violazioni di dati personali possono accadere per un ampio numero di ragioni che possono includere:

1. Divulgazione di dati personali a soggetti non autorizzati;
2. Perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
3. Perdita o furto di documenti cartacei;
4. Infedeltà aziendale (ad esempio: data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico);
5. Accesso abusivo (ad esempio: data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
6. Casi di pirateria informatica (usurpazione delle credenziali di accesso/fishing);
7. Banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "owner";
8. Virus o altri attacchi al sistema informatico o alla rete aziendale;
9. Violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o armadi contenenti archivi con informazioni riservate);
10. Smarrimento di pc portatili, devices o attrezzature informatiche di proprietà dell'Istituto;
11. Invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

A CHI SONO RIVOLTE QUESTE PROCEDURE?

Queste procedure sono rivolte a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del Titolare del trattamento (meglio descritti al punto 5 della presente procedura) quali:

a) I lavoratori dipendenti, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto contrattuale intercorrente - abbiano accesso ai dati personali trattati nel corso delle prestazioni richieste per conto del Titolare del trattamento;

b) qualsiasi soggetto (persona fisica o persona giuridica) diverso dal Destinatario interno che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento (art. 28 GDPR) o di autonomo Titolare;

Il rispetto della presente procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia.

A QUALI TIPI DI DATI SI RIFEREISCE QUESTA PROCEDURA

Queste procedure si riferiscono a:

- Dati personali trattati "da" e "per conto" del Titolare del trattamento, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo;
- Dati personali conservati o trattati a mezzo di qualsiasi altro sistema nell'Istituto.

Per «dato personale» si intende: 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.

GESTIONE COMUNICAZIONE DI DATABREACHES

Le violazioni di dati personali sono gestite dal Titolare del trattamento o da un suo delegato, sotto la supervisione del DPO.

In caso di concreta, sospetta e/o avvenuta violazione dei dati personali, è di estrema importanza assicurare che la stessa sia affrontata immediatamente e correttamente al fine di minimizzare l'impatto della violazione e prevenire che si ripeta.

Nel caso in cui uno dei Destinatari si accorga di una concreta, potenziale o sospetta violazione dei dati personali, dovrà immediatamente informare dell'incidente il superiore gerarchico, il quale si occuperà, con il supporto dei Destinatari stessi, di informare il Titolare del trattamento o un suo delegato mediante la compilazione dell'Allegato A – Modulo di comunicazione interna di Data Breach da inviare a mezzo mail all'indirizzo: dpo@icgrosseto6.edu.it

GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI

Per gestire una violazione dei dati personali è necessario seguire i seguenti cinque passaggi, di cui due eventuali:

Step 1: Identificazione e indagine preliminare;

Step 2: Contenimento, recovery e risk assessment;

Step 3: Notifica all'Autorità Garante (eventuale);

Step 4: Comunicazione agli interessati (eventuale)

;Step 5: Documentazione della violazione;

Step 1: Identificazione e indagine preliminare

L'Allegato A, debitamente compilato, permetterà al Titolare del trattamento o un suo delegato, di condurre una valutazione iniziale riguardante la notizia dell'incidente occorso, ciò al fine di stabilire se si sia effettivamente verificata un'ipotesi di Data Breach (violazione) e se sia necessaria un'indagine più approfondita dell'accaduto, procedendo con il risk assessment (step 2) e con il coinvolgimento del DPO

Nel caso in cui si tratti di violazione di dati contenuti in un sistema informatico, il Titolare del trattamento o un

suo delegato dovrà coinvolgerein tutta la procedura indicata nel presente documento anche il Responsabile dell'Area IT o un suo delegato in caso di assenza.

Detta valutazione iniziale sarà effettuata attraverso l'esame delle informazioni riportate nell'Allegato A, quali:

- la data di scoperta della violazione (tempestività);
- Il soggetto che è venuto a conoscenza della violazione;
- la descrizione dell'incidente (natura della violazione e dei dati coinvolti);
- le categorie e il numero approssimativo degli interessati coinvolti nella violazione;
- la descrizione di eventuali azioni già poste in essere.

Step 2: Contenimento, Recovery e risk assessment

Una volta stabilito che un Data Breach è avvenuto, il Titolare del trattamento o un suo delegato insieme al DPO dovranno stabilire:

- se esistono azioni che possano limitare i danni che la violazione potrebbe causare (i.e. riparazione fisica di strumentazione; utilizzo dei file di back up per recuperare dati persi o danneggiati; isolamento/chiusura di un settore compromesso della rete; cambio dei codici di accesso… ecc.);
- una volta identificate tali azioni, quali siano i soggetti che devono agire per contenere la violazione;
- se sia necessario notificare la violazione all'Autorità Garante per la Protezione dei dati personali (ove sia probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche);
- se sia necessario comunicare la violazione agli interessati (ove la violazione presenti un elevato rischio per i diritti e le libertà delle persone fisiche).

Al fine di individuare la necessità di notificazione all'Autorità Garante e di comunicazione agli interessati, il Titolare del trattamento e il DPO valuteranno la gravità della violazione utilizzando l'Allegato B - Modulo di valutazione del Rischio connesso al Data Breach che dovrà essere esaminato unitamente all'Allegato A, tenendo, altresì, in debita considerazione i principi e le indicazioni di cui all'art. 33 GDPR .

Se, infatti, gli obblighi di notifica all'Autorità di Controllo scaturiscono dal superamento di una soglia di rischio semplice, l'art. 34 GDPR prevede, invece, che l'obbligo di comunicazione agli interessati sia innescato dal superamento di un rischio elevato.

Step 3: Notifica all'Autorità Garante competente (eventuale)

Una volta valutata la necessità di effettuare notifica della violazione dei dati subita, sulla base della procedura di cui allo step 2, secondo quanto prescritto dal Regolamento (UE) 2016/679, l'Istituto Comprensivo Grosseto 6 provvederà, senza ingiustificato ritardo e, ove possibile entro 72 ore dal momento in cui ne è venuta a conoscenza.
Pertanto, il Titolare del trattamento e il DPO individueranno la corretta modulistica da utilizzare per effettuare la notificazione e vi provvederanno.

Step 4: Comunicazione agli interessati (eventuale)

Una volta valutata la necessità di effettuare la comunicazione della violazione dei dati agli interessati, sulla base della procedura di cui allo step 2, secondo quanto prescritto dal Regolamento (UE) 2016/679, l'Istituto Comprensivo Grosseto 6 dovrà provvedervi, senza ingiustificato ritardo.
Quanto al contenuto di tale comunicazione, il Titolare del trattamento o un suo delegato e il DPO dovranno:

- comunicare il nome e i dati di contatto del Responsabile della protezione dei dati (DPO);
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte delTitolare del trattamento per porre rimedio alla violazione dei dati personali e, se del caso, per attenuarne i possibili effetti negativi.

Quanto alle modalità di comunicazione, caso per caso, il Titolare del trattamento o un suo delegato e il DPO dovranno sempre privilegiare la modalità di comunicazione diretta con i soggetti interessati (quali e- mail, SMS

o messaggi diretti). Il messaggio dovrà essere comunicato in maniera evidente e trasparente, evitando quindi di inviare le informazioni nel contesto di update generali o newsletter, che potrebbero essere facilmente fraintesi dai lettori. Nel caso in cui la segnalazione diretta richieda uno sforzo ritenuto sproporzionato, allora si potrà utilizzare una comunicazione pubblica, che dovrà essere ugualmente efficace nel contatto diretto con l'interessato.

Step 5: Documentazione della violazione

Indipendentemente dalla valutazione circa la necessità di procedere a notificazione e/o comunicazione della violazione di Data Breach, ogni qualvolta si verifichi un incidente comunicato dai Destinatari attraverso l'Allegato A, l'Istituto Comprensivo Grosseto 6 sarà tenuto a documentarlo. Tale documentazione sarà affidata al Titolare del trattamento o da un suo delegato con l'ausilio del Responsabile dell'Ufficio IT (qualora la violazione riguardi dati contenuti in sistemi informatici) vi provvederà mediante la tenuta del Registro dei Data Breach, secondo le informazioni ivi riportate:

(i) n. violazione;
(ii) data violazione;
(iii) natura della violazione;
(iv) categoria di interessati;
(v) categoria di dati personali coinvolti;
(vi) numeroapprossimativo di registrazioni dei dati personali;
(vii) conseguenze della violazione; (viii) contromisure adottate;
(viii) se sia stata effettuata notifica all'Autorità Garante Privacy;
(ix) se sia stata effettuata comunicazione agli interessati.

Il Registro dei Data Breach deve essere continuamente aggiornato e messo a disposizione del Garante, qualora l'Autorità chieda di accedervi.

ALLEGATO A – MODULO DI COMUNICAZIONE DATA BREACH

Qualora scopra un Data Breach, è pregato di informare immediatamente ilSuo superiore gerarchico, il quale, a sua volta, dovrà compilare la modulistica a seguire e inviarla a mezzo e-mail al seguente indirizzo email: dpo@icgrosseto6.edu.it

Comunicazione di Data Breach	**Note**
Data scoperta violazione:	
Data dell'incidente:	
Luogo della violazione (specificare se sia avvenuta a seguito di smarrimento di dispositivio di supporti portatili):	
Nome della persona che ha riferito della violazione:	
Dati di contatto della persona che ha riferito della violazione (indirizzo e-mail, numero telefonico): *In caso di destinatario esterno indicare la ragione sociale:*	
Denominazione della/e banca/che dati oggetto di Data Breach e breve descrizione della violazionedei dati personali ivi trattati:	
Categorie e numero approssimativo di interessati coinvolti nella violazione:	
Breve descrizione di eventuali azioni attuate al momento della scoperta della violazione:	
Responsabile della struttura:	
data:	

ALLEGATO B – MODULO DI VALUTAZIONE DEL RISCHIO CONNESSO AL DATA BREACH

Assessment di gravità	**A cura del DPO insieme con Amministratore di sistema (se del caso) e il Responsabile dell'ufficio coinvolto della violazione**
Dispositivi oggetto del Data Breach (computer, rete dispositivo mobile, file o parte di un file, strumento di back up, documento cartaceo, altro).	
Modalità di esposizione al rischio (tipo di violazione): lettura (presumibilmente i dati non sono stati copiati), copia (i dati sono ancora presenti sui sistemi ma del titolare), alterazione (i dati sono presenti sui sistemi ma sono stati alterati), cancellazione (i dati non sono più presenti e non li ha neppure l'autore della violazione), furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione), altro.	
Breve descrizione dei sistemi di elaborazione o di memorizzazione dati coinvolti, con indicazionedella loro ubicazione.	
Se laptop è stato perso/rubato: quando è stata l'ultima volta in cui il laptop è stato sincronizzato con il sistema IT centrale?	
Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati violata?	
La violazione può avere conseguenze negative in uno dei seguenti settori aziendali: operation, research, financial, legal, liability or reputation?	
Qual è la natura dei dati coinvolti? Compilare le sezioni sottostanti:	

a. Dati personali generici	
b. I dati particolari (come identificati dal Regolamento (UE) 2016/679 relative ad una persona viva ed individuabile: ▪ origine razziale o etnica; ▪ opinion politiche, convinzioni religiose o filosofiche; ▪ appartenenza sindacale; ▪ dati genetici; ▪ dati biometrici; ▪ dati giudiziari; ▪ relative alla salute o all'orientamento sessuale di una persona.	
c. Informazioni che possono essere utilizzate per commettere furti d'identità (i.e. dati di accesso e di identificazione, codice fiscale e copie di carta d'identità, passaporto o carte di credito);	
d. Informazioni personali relative a soggetti fragili (i.e. anziani, disabili, minori);	
e. Profili individuali che includono informazioni relative a performance lavorative, salario o stato di famiglia, sanzioni disciplinari, che potrebbero causare danni significativi alle persone;	
Altro:	
La violazione può comportare pregiudizio alla reputazione, perdita di riservatezza di dati protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro dato economico o sociale significativo?	
Gli interessati rischiano di essere privati dell'esercizio del controllo sui dati personali cheli riguardano?	
Quali misure tecniche e organizzative sono adottateai dati oggetto di violazione? (i.e. La pseudonimizzazione e la cifratura dei dati personali)	
Il Titolare del trattamento ha adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati successivamente alla violazione?	
Classificazione della violazione (1, 2 o 3) e motivazioni:	

Notificazione del Data Breach all'Autorità Garante	Si/NO Se sì, notificato in data: Dettagli:
Comunicazione del Data Breach agli interessati	Si/NO Se sì, notificato in data: Dettagli:
Comunicazione del Data Breach ad altri soggetti	Si/NO Se sì, notificato in data: Dettagli: