DATA BREACH POLICY

PROCEDURE OPERATIVE IN CASO DI VIOLAZIONE DEI DATI PERSONALI

INDICE

1. PREMESSA 3
2. SCOPO 3
3. AMBITO DI APPLICAZIONE 3
4. DESTINATARI 4
5. SEGNALAZIONE DELLA VIOLAZIONE 5
6. GESTIONE DELLA VIOLAZIONE 5

Identificazione dell'incidente ed indagine preliminare 5

Contenimento, *recovery* e *risk assessment* 6

Notifica al Garante 6

Comunicazione agli interessati 7

Registrazione della violazione 7

ALLEGATI:

A – Modulo per la segnalazione della violazione dei dati – *data breach* 8

B – Registro delle violazioni dei dati personali – *data breaches* 10

1. PREMESSA

Quale titolare del trattamento, questa istituzione scolastica è tenuta, ai sensi del Regolamento Europeo 2016/679 (da qui in avanti "GDPR"), a proteggere i dati personali che tratta nello svolgimento delle proprie attività istituzionali apprestando misure tecniche e organizzative adeguate, e ad agire senza ingiustificato ritardo nel caso in cui si verifichi – nonostante tali misure di sicurezza – una violazione dei dati stessi (*data breach*).

L'art. 33 del GDPR impone infatti al titolare del trattamento di notificare la violazione all'Autorità di controllo (Garante per la protezione dei dati personali, da qui in avanti "Garante") entro 72 ore dal momento in cui ne viene a conoscenza.

All'obbligo di notifica al Garante – che scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche – si aggiunge, se tale rischio risulti elevato, l'obbligo di effettuare senza ingiustificato ritardo la comunicazione della violazione dei dati nei confronti degli interessati (art. 34).

L'eventuale inadempimento di tali obblighi esporrebbe questa istituzione scolastica alle conseguenze dell'esercizio da parte dell'Autorità di controllo, dei poteri che le attribuisce l'art. 58 del GDPR, o alle sanzioni stabilite dall'art. 83.

Essendo pertanto di fondamentale importanza predisporre azioni da attuare con tempestività laddove vengano riscontrate violazioni di dati personali, questa istituzione scolastica, in persona del suo legale rappresentante, ha ritenuto di adottare le presenti procedure operative.

2. SCOPO

Lo scopo della presenti procedure è quello di fornire al personale scolastico le istruzioni operative necessarie per la gestione delle violazioni dei dati personali, descrivendo, in un flusso procedurale, tutti i passaggi da seguire, dalla prima rilevazione della violazione sino alla definitiva chiusura della relativa procedura, nel caso in cui si verifichi un incidente della sicurezza dei dati.

3. AMBITO DI APPLICAZIONE

L'art. 4, n. 12), del GDPR definisce "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".

In pratica, una violazione dei dati personali (*data breach*) si verifica quando ne viene violata la confidenzialità, l'integrità, la disponibilità (i tre pilastri sui quali poggia la corretta gestione e protezione dei dati).

Alcuni possibili esempi di *data breach* sono i seguenti:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;

- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

In generale, le possibili cause di *data breach* sono riconducibili a tre macro aree[1]: 1) comportamenti degli operatori (furto o smarrimento di credenziali di autenticazione; carenza di consapevolezza, disattenzione o incuria; condotte sleali o fraudolente; errori materiali); 2) eventi relativi agli strumenti informatici (azione di virus o software malevoli; spamming o altre tecniche di sabotaggio; malfunzionamento, indisponibilità o degrado degli strumenti; accessi dall'esterno, non autorizzati; intercettazione di informazioni in rete); 3) eventi relativi al contesto (accessi non autorizzati a locali/reparti interni ad accesso ristretto; furto di strumenti contenenti dati; eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria; guasto ai sistemi complementari come l'impianto elettrico o di climatizzazione; errori umani nella gestione della sicurezza fisica).

Costituisce "dato personale" (ai sensi dell'art. 4, n. 1), del GDPR) "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.".

Le presenti procedure si riferiscono a tutti i dati personali trattati "dal" o "per conto del" titolare del trattamento, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo, ed a qualunque tipo di violazione che li riguardi.

4. DESTINATARI

Le istruzioni operative contenute nelle presenti procedure operative sono rivolte a tutti i soggetti che, a qualunque titolo, trattano dati personali (di studenti e genitori, docenti, a.t.a., fornitori, ecc.) di competenza di questa istituzione scolastica titolare del trattamento, come ad esempio:

- il personale scolastico (a prescindere dalla tipologia di rapporto individuale di lavoro e dal relativo inquadramento) che ha accesso a tali dati personali e su di essi effettua operazioni di trattamento nello svolgimento delle proprie mansioni (di seguito genericamente denominati "destinatari interni");

- qualsiasi persona fisica (diversa dal destinatario interno) o persona giuridica che sugli stessi dati effettua un trattamento per conto di questa istituzione scolastica e pertanto agisce in qualità di responsabile del trattamento ai sensi dell'art. 28 del GDPR, ovvero che li tratta quale autonomo titolare (di seguito genericamente denominati "destinatari esterni").

Tutti i destinatari devono essere debitamente informati dell'adozione delle presenti procedure.

Il rispetto delle presenti procedure è obbligatorio per tutti i destinatari e la violazione delle istruzioni operative in esse contenute può comportare, a seconda dei casi e salvo eventuali conseguenze più gravi previste dalla legge, provvedimenti disciplinari a carico dei dipendenti ovvero la risoluzione dei

[1] In base alla classificazione che, redatta a suo tempo dal Garante ("Prime riflessioni sui criteri di redazione del Documento Programmatico sulla Sicurezza", del 13 maggio 2004) appare ancora attuale, ancorché eventualmente integrabile in considerazione del progresso tecnologico.

contratti in essere con il destinatario esterno inadempiente.

5. SEGNALAZIONE DELLA VIOLAZIONE

Le violazioni dei dati personali sono gestite dal titolare del trattamento, sotto la supervisione del responsabile della protezione dei dati (da qui in avanti "DPO").

In tal caso è di estrema importanza adoperarsi affinché esse vengano affrontate con tempestività ed adeguatezza, al fine di contenerne i rischi e le conseguenze per l'interessato, e, se possibile, di eliminare le cause che le hanno determinate o di adottare le misure tecniche ed organizzative necessarie per impedire che possano ripetersi.

Chiunque rilevi una violazione dei dati personali dovrà pertanto denunciarla immediatamente al Dirigente Scolastico, compilando in ogni sua parte l'allegato "Modulo per la segnalazione della violazione dei dati – *data breach*" (allegato "A") e consegnandolo personalmente o inviandolo per posta elettronica all'indirizzo e-mail istituzionale.

6. GESTIONE DELLA VIOLAZIONE

La gestione della violazione dei dati personali avviene attraverso 5 interventi:

1) identificazione dell'incidente ed indagine preliminare;
2) contenimento, *recovery* e *risk assessment*;
3) eventuale notifica all'Autorità Garante;
4) eventuale comunicazione agli interessati;
5) documentazione della violazione.

1) Identificazione e indagine preliminare

L'allegato "Modulo per la segnalazione della violazione dei dati – *data breach*" (elaborato in base al "Modello di notifica al Garante"), se correttamente compilato da chi effettua la segnalazione, consente al titolare del trattamento di effettuare una prima valutazione in ordine alla notizia dell'incidente portato alla sua conoscenza.

Ciò è necessario al fine di stabilire se quanto viene denunciato configura effettivamente una ipotesi di *data breach*, ossia una violazione della sicurezza dei dati personali, e se richiede di effettuare una valutazione della gravità del rischio (*risk assessment*) con il coinvolgimento del DPO.

Nel caso in cui si tratti di violazione di dati contenuti nel sistema informatico, il titolare del trattamento dovrà coinvolgere in tutte le procedure indicate nel presente documento anche l'amministratore di sistema (se nominato).

Tale valutazione iniziale sarà effettuata attraverso l'esame delle informazioni riportate nell'allegato "A", quali:

- data di scoperta e denuncia della violazione;
- natura e cause della violazione;
- tipologia e volume dei dati personali violati;
- categorie e numero approssimativo di interessati coinvolti nella violazione;

- eventuali azioni spontanee già poste in essere dal denunciante per fronteggiare la violazione.

2) Contenimento, *recovery* e *risk assessment*

Accertato che l'oggetto della segnalazione effettivamente configura un caso di *data breach*, il titolare del trattamento ed il DPO (eventualmente, con l'amministratore di sistema) dovranno valutare e stabilire:

- le azioni da intraprendere per contenere i danni che la violazione potrebbe causare (come ad esempio: l'utilizzo dei file di backup per recuperare i dati persi o danneggiati; l'isolamento/chiusura di un settore compromesso della rete; il cambio dei codici di accesso; la riparazione fisica di un dispositivo danneggiato; ecc.);
- i soggetti che devono eseguire gli interventi di contenimento;
- se sia necessario notificare la violazione al Garante (nel caso in cui è probabile che la violazione dei dati personali 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 rischio elevato per i diritti e le libertà delle persone fisiche).

Al fine di individuare la necessità della notificazione al Garante e della comunicazione agli interessati, il titolare del trattamento ed il DPO effettueranno una valutazione della gravità della violazione (*risk assessment*), esaminandone le risultanze unitamente alle altre circostanze segnalate nell'allegato "A" e tenendo altresì in debita considerazione i principi e le indicazioni di cui agli artt. 33 e 34 del GDPR.

L'obbligo di notifica al Garante scaturisce dal superamento di una soglia di rischio semplice, mentre l'art. 34 del GDPR prevede invece che l'obbligo di comunicazione agli interessati sia innescato solo dal superamento di un rischio elevato.

I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;
- comprendere dati che possono accrescere ulteriormente i potenziali rischi (es. dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un'elevata probabilità di accadimento (es. rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (es. pazienti, minori, soggetti indagati).

3) Eventuale notifica al Garante

Se all'esito delle precedenti valutazioni risulta obbligatoria la notifica della violazione subita, il titolare del trattamento vi provvede senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuta a conoscenza, utilizzando l'apposita modulistica disponibile sul sito internet del Garante (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-

display/docweb/9128501), che deve essere sottoscritta digitalmente (con firma elettronica qualificata/firma digitale) ovvero con firma autografa; in quest'ultimo caso la notifica deve essere presentata unitamente alla copia del documento d'identità del firmatario.

L'invio della notifica al Garante va effettuato tramite posta elettronica certificata all'indirizzo protocollo@pec.gpdp.it oppure tramite posta elettronica ordinaria all'indirizzo protocollo@gpdp.it, ovvero, attraverso l'apposita procedura online che il Garante avrà reso disponibile.

4) Eventuale comunicazione agli interessati

Se all'esito delle valutazioni di *risk assesment* emerge la necessità di effettuare la comunicazione della violazione dei dati agli interessati e non ricorrono le condizioni di cui all'art. 34, par. 2, del GDPR, il titolare del trattamento vi provvede senza ingiustificato ritardo.

Tale comunicazione deve contenere:

- il nome e i dati di contatto del DPO;
- la descrizione delle probabili conseguenze della violazione dei dati personali;
- la 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, se del caso, per attenuarne i possibili effetti negativi.

Nel caso in cui la comunicazione della violazione agli interessati richiederebbe sforzi sproporzionati, si può procedere ad una comunicazione pubblica (o a una misura simile) tramite la quale informare con analoga efficacia gli interessati.

5) Documentazione della violazione

Indipendentemente dalla valutazioni raggiunte in ordine alla necessità della notificazione e della comunicazione della violazione dei dati personali, se l'incidente segnalato attraverso l'allegato A configura un caso di *data breach* esso andrà documentato da parte del titolare del trattamento (con l'eventuale ausilio dell'amministratore di sistema qualora la violazione riguardi dati contenuti in sistemi informatici), mediante annotazione nell'apposito "Registro delle violazioni dei dati personali *(data breaches)* (Allegato "B") per consentire eventuali verifiche da parte del Garante.

Il presente documento comprende **2 allegati:**

A – Modulo per la segnalazione della violazione dei dati – *data breach*;
B – Registro delle violazioni dei dati personali (*data breaches*).

Allegato "A"

MODULO PER LA SEGNALAZIONE DELLA VIOLAZIONE DEI DATI – *DATA BREACH*

(elaborato in base al Modello di notifica al Garante)

Al Dirigente Scolastico

Il/la sottoscritto/a_____,

- in servizio presso questa Istituzione scolastica con la qualifica di_____;
- soggetto esterno rispetto a questa Istituzione scolastica_____;

nominato/a, in relazione al trattamento dei dati personali, quale

- autorizzato;
- designato;
- responsabile;
- altro (specificare):_____,

segnala

di essere venuto a conoscenza il giorno___/___/20___alle ore___,___,

- direttamente, attraverso_____;
- da parte di_____;

che

- il giorno___/___/20___;
- dal___/___/20___ore___,___(se la violazione è ancora in corso);
- dal___/___/20___ore___,___al___/___/20___ore___,___;
- in un tempo che non è in grado di determinare_____;

si è verificata la seguente violazione dei dati personali trattati da questa Istituzione scolastica

(descrivere) _____
_____;

tale violazione attiene alla

- confidenzialità dei dati (divulgazione, diffusione, accesso non autorizzato o accidentale);
- integrità dei dati (alterazione o modifica non autorizzata o accidentale);
- disponibilità dei dati (impossibilità di accesso, perdita, distruzione non autorizzata o accidentale),

ed è conseguente a

- azione intenzionale interna (attribuibile a_____);
- azione accidentale interna (attribuibile a_____);
- azione intenzionale esterna (attribuibile a_____);
- azione accidentale esterna (attribuibile a_____);
- sconosciuta;
- altro (specificare)_____);

i dati personali che sono stati oggetto di violazione appartengono alle seguenti categorie

- dati anagrafici (nome, cognome, data di nascita, luogo di nascita, codice fiscale, ecc.);
- dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile);
- dati di accesso e di identificazione (username, password, ecc.);

- dati di pagamento (numero di conto corrente, dettagli della carta di credito, ecc.);
- dati relativi alla fornitura di un servizio di comunicazione elettronica (traffico, navigazione internet, ecc.);
- dati relativi a condanne penali e ai reati o a connesse misure di sicurezza o di prevenzione;
- dati di profilazione;
- dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, ecc.);
- dati di localizzazione
- dati che rivelano l'origine razziale o etnica;
- dati che rivelano le opinioni politiche;
- dati che rivelano le convinzioni religiose o filosofiche;
- dati che rivelano l'appartenenza sindacale;
- dati relativi alla vita sessuale o all'orientamento sessuale;
- dati relativi alla salute;
- dati genetici;
- dati biometrici;
- categorie non ancora determinate;
- altro (specificare)_____;

il volume (anche approssimativo) dei dati personali violati
(numero di documenti, files, records di database, transazioni registrate, ecc.) corrisponde a

- n°_____;
- circa n°_____;
- un numero (ancora) non definito di dati;

i dati violati appartengono alle seguenti categorie di interessati

- dipendenti/consulenti/collaboratori, ecc.;
- studenti maggiorenni;
- studenti minorenni;
- genitori/familiari di studenti;
- categorie (non ancora) determinate;
- altro (specificare)_____;

il numero (anche approssimativo) degli interessati coinvolti nella violazione corrisponde a

- n°_____;
- circa n°_____;
- un numero (ancora) sconosciuto;

le informazioni di dettaglio sulla violazione che è possibile aggiungere sono

- descrizione dell'incidente di sicurezza alla base della violazione_____
_____;
- descrizione dei sistemi e delle infrastrutture IT coinvolti nell'incidente (con indicazione della loro ubicazione)
_____;
- descrizione delle misure di sicurezza tecniche e organizzative che erano state adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture IT coinvolti nell'incidente _____
_____;

le azioni spontanee già poste in essere per fronteggiare la violazione sono

(descrivere)_____;

i dati di contatto per eventuali chiarimenti o informazioni ulteriori sono

telefono cellulare_____; telefono fisso_____; e-mail_____.

(Luogo e data)_____,____/____/20____

(Firma) _____