PROCEDURA PER DATA BREACH

Definizioni

La presente procedura è adottata dall'Istituto Niccolini Palli di Livorno con sede legale in Livorno, Via E. Rossi 6. Il Titolare del Trattamento, Dirigente Scolastica Dott.ssa Teresa Cini ha nominato quale responsabile del trattamento il Direttore dei Servizi Generali Amministrativi, Dott. Alessandro Raffaele e quale Responsabile della Protezione dei Dati (DPO) l'Avv. Chiara Giannessi.

Ai fini della presente procedura, valgono le seguenti definizioni:

a) 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".

b) 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 ai sensi dell'art. 28 GDPR".

c) Incaricato del trattamento: "La persona fisica che nell'ambito della struttura aziendale del Titolare è autorizzata a effettuare attività di trattamento di dati personali".

d) RPD/DPO: "Il Responsabile del trattamento come individuato dalla Sezione 4 (artt. 37-39) del Regolamento (UE) n. 2016/679".

e) Dato personale: "Qualunque informazione relativa a persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare 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, generica, psichica, economica, culturale o sociale".

f) 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".

La gestione dei data breach

Ai sensi dell'art. 33 del Regolamento (UE) n. 2016/679, il Titolare del trattamento, in caso sia consapevole di una violazione dei Dati personali trattati, è tenuto:

- a informare l'Autorità di controllo (il Garante per la protezione dei dati personali, nel caso del territorio italiano) entro e non oltre le 72 ore - preferibile il rispetto del termine delle 48 ore indicato nel Provvedimento del Garante del 2 luglio 2015 - successive all'avvenuta conoscenza della violazione. Si precisa che il Titolare non è tenuto alla notifica se sia improbabile che la violazione dei Dati personali presenti un rischio per i diritti e le libertà degli Interessati;
- nel caso in cui tale violazione sia suscettibile di comportare un rischio elevato per i diritti e le libertà degli interessati, a informare senza ritardo anche gli stessi Interessati.

A tal fine, il Titolare del trattamento, come sopra identificato, ha previsto un apposito processo per la gestione e la notifica in caso di Data Breach.

Al fine di rendere effettivo il processo di notifica, è altresì importante che tutti coloro che nell'ambito del rapporto di lavoro e/o di collaborazione trattano Dati personali del Titolare del trattamento siano previamente sensibilizzati e partecipino attivamente a tale processo, segnalando tempestivamente ogni caso di violazione di cui siano venuti a conoscenza e ogni evento che potrebbe potenzialmente condurre ad una violazione.

Data Breach e potenziali scenari

Il GDPR definisce violazione dei dati personali o Data Breach "*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*" (art. 4, n. 12). Le indicazioni di cui alla presente sezione della Procedura valgono per qualsiasi tipologia di Dato personale.

Eventi di Data Breach possono riguardare sia casi cui è connesso un rischio marginale (es. perdita di una chiavetta USB di un dipendente), che casi più critici di furto o perdita di intere basi dati, quali, a titolo esemplificativo, le banche dati gestite dal Titolare del trattamento.

Nel caso si verificasse una delle casistiche riportate di seguito, o un analogo scenario, è fondamentale chiedersi se e quale tipo di Dati personali sono coinvolti nell'evento, e, di conseguenza, procedere alla segnalazione:

- ✓ furto o smarrimento di laptop, smartphone, tablet aziendali contenenti Dati personali;
- ✓ furto o smarrimento di documenti cartacei contenenti Dati personali;
- ✓ furto o smarrimento di dispositivi portatili di archiviazione non criptati, come chiavette USB e hard disk esterni, contenenti Dati personali;
- ✓ perdita o modifica irreparabile di archivi contenenti Dati personali in formato cartaceo o digitale (ad esempio, a causa di una errata cancellazione o modifica dai sistemi o dagli archivi digitali aziendali che non possa essere ripristinata attraverso l'uso di un backup);
- ✓ diffusione impropria di Dati personali, per mezzo di:
    - o invio di e-mail contenente Dati personali al destinatario errato;
    - o invio di e-mail con un file contenente Dati personali allegato erroneamente;
    - o esportazione fraudolenta o errata di Dati personali dai sistemi aziendali;
    - o richiesta di invio di documenti e file contenenti Dati personali da parte di un esterno che si finge fraudolentemente un collega, collaboratore e/o altro soggetto e conseguente invio allo stesso di tali documenti e file;
- ✓ segnalazione da parte di un fornitore di un evento di Data Breach sui propri sistemi che ha interessato o potrebbe potenzialmente interessare Dati personali del Titolare del trattamento.

Processo di gestione del Data Breach

Al fine di consentire una gestione efficace e tempestiva delle violazioni dei Dati personali, il Titolare del trattamento adotta un processo strutturato per la gestione dei casi di Data Breach che prevede:

- ✓ Rilevazione e segnalazione del Data Breach;
- ✓ Analisi del Data Breach;
- ✓ Risposta e notifica del Data Breach;

- ✓ Registrazione del Data Breach.

Rilevazione e segnalazione del Data Breach

La rilevazione e segnalazione del Data Breach è un obbligo per tutti i dipendenti e/o collaboratori del Titolare del trattamento.

Nel caso in cui si verifichi uno degli eventi sopradescritti descritti o in tutti gli altri casi in cui il soggetto che tratta dati personali sia consapevole di altri eventi potenzialmente rischiosi per i documenti e gli archivi, è tenuto a informare immediatamente il Dirigente Scolastico il quale provvede – senza indugio – a darne notizia al Responsabile per la Protezione dei Dati personali (DPO).

Nel caso di un incidente informatico, dovrà essere compilata la scheda su apposito registro informatico la cui struttura è allegata al presente atto (ALLEGATO 1). Al registro andranno allegate tutte le comunicazioni relative all'incidente (ad es. denuncia all'autorità giudiziaria, notifica al Garante Privacy e relativa corrispondenza, comunicazioni agli interessati, ecc.).

In tale Registro dovranno essere inseriti tutti gli eventi che determinano o configurano anomalie rispetto alla normale gestione dei sistemi informatici (ad esempio: Virus, perdita di dati, alterazione di dati, attacchi alla rete, furti di credenziali, ecc.).

Analisi del Data Breach

A seguito della rilevazione e/o segnalazione, il Dirigente Scolastico – sentito il Responsabile per la protezione dei dati personali - effettua una valutazione al fine di verificare che nell'incidente rilevato siano stati effettivamente violati Dati personali trattati dall'Istituto.

La suddetta analisi è finalizzata alla raccolta ed identificazione delle seguenti informazioni:

- ✓ categorie di Interessati cui i Dati personali violati si riferiscono (ad esempio, utenti, dipendenti, fornitori, etc.);
- ✓ categorie di Dati personali compromessi (ad esempio, Dati personali, Dati sensibili, Dati giudiziari);
- ✓ tipologia di Data Breach: violazione della riservatezza, disponibilità o integrità (ad esempio, accesso non autorizzato, perdita, alterazione, furto, *disclosure*, distruzione, etc.).

Nell'ambito di tale analisi, il Titolare del trattamento – con il supporto del DPO - identifica le azioni di prima risposta da intraprendere nell'immediato per contenere gli impatti della violazione dei Dati personali.

Nell'ambito dell'analisi della violazione, vengono identificate anche le seguenti informazioni:

- ✓ identificabilità degli Interessati i cui dati rappresentano l'oggetto della violazione;
- ✓ misure di sicurezza tecniche e organizzative che potrebbero aver parzialmente o *in toto* mitigato gli impatti relativi al Data Breach;
- ✓ ritardi nella rilevazione del Data Breach;
- ✓ numero di individui interessati.

Sulla base dei suddetti parametri, il Titolare del trattamento competente procede alla valutazione della gravità del Data Breach relativamente ai diritti ed alle libertà degli Interessati, a seconda della natura dei Dati personali (ad esempio, Dati particolarmente sensibili e/o giudiziari), delle misure di sicurezza adottate, della tipologia di interessati (ad esempio, minori o altri soggetti vulnerabili).

Risposta e notifica del Data Breach

La precedente fase di analisi fornisce al Titolare del trattamento gli strumenti necessari a identificare e valutare le conseguenze negative e gli impatti causati dalla violazione di Dati personali rilevata.

Nel caso in cui dovesse risultare improbabile che il Data Breach presenti rischi per i diritti e le libertà degli interessati, la notifica all'Autorità Garante risulta essere non obbligatoria. Tale valutazione è condivisa con il DPO.

Qualora al contrario dovesse risultare possibile che il Data Breach presenti rischi per i diritti e le libertà degli Interessati, il Dirigente Scolastico, con il supporto del DPO, deve procedere a predisporre la notifica all'Autorità Garante secondo il modello allegato al presente atto (ALLEGATO 2).

La notifica viene effettuata all'Autorità Garante entro 72 ore dal momento in cui il Data Breach è stato rilevato.

La suddetta notifica contiene almeno le seguenti informazioni:

- ✓ natura della violazione dei dati personali (*disclosure*, perdita, alterazione, accesso non autorizzato, etc.);

- ✓ tipologie di Dati personali violati;
- ✓ categorie e numero approssimativo di Interessati cui i dati compromessi si riferiscono;
- ✓ nome e dati di contatto del DPO, che sarà l'interfaccia per Titolare del trattamento nei confronti dell'Autorità di controllo;
- ✓ probabili conseguenze della violazione dei Dati personali;
- ✓ descrizione delle misure che il Titolare del trattamento ha adottato o è in procinto di adottare al fine di mitigare le conseguenze del Data Breach;
- ✓ ove la stessa non sia presentata entro 48/72 ore dalla rilevazione, i motivi dell'eventuale ritardo nella comunicazione.

Qualora non sia stato possibile fornire contestualmente tutte le informazioni obbligatorie, il Dirigente Scolastico raccoglie quanto prima le informazioni supplementari e provvede a integrare, senza ritardo, la notifica già inoltrata all'Autorità di Controllo.

Oltre a notificare il Data Breach all'Autorità Garante, il Titolare del trattamento è tenuto a valutare l'esigenza di procedere con la denuncia all'Autorità Giudiziaria competente, nonché con la notifica del Data Breach anche ai soggetti interessati i cui dati siano stati violati.

Per stabilire se sia necessario provvedere alla notifica agli Interessati, il Titolare del trattamento, di concerto con il DPO, deve valutare i seguenti fattori:

- ✓ il trattamento può comportare discriminazioni, furto d'identità, perdite finanziare, disturbi psicologici, pregiudizio alla reputazione, perdita di riservatezza dei Dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo;
- ✓ gli Interessati rischiano di essere privati dei loro diritti, delle libertà o venga loro impedito l'esercizio del controllo sui Dati personali che li riguardano;
- ✓ sono trattati Dati personali che rivelano l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi a condanne penali e a reati o alle relative misure di sicurezza;
- ✓ in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali,

l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;

- ✓ sono trattati Dati personali di persone fisiche vulnerabili, in particolare minori;
- ✓ il trattamento riguarda una notevole quantità di Dati personali e un vasto numero di Interessati.

La notifica agli Interessati deve, pertanto, avvenire nel caso in cui la violazione di Dati personali presenti un rischio elevato per i diritti e le libertà delle persone fisiche, a meno che non sia verificata almeno una delle seguenti condizioni:

- ✓ sono state applicate adeguate misure tecniche e organizzative per proteggere i dati prima della violazione, in particolare quelle in grado di renderle non intelligibili per soggetti terzi non autorizzati (ad esempio, misure di cifratura);
- ✓ a valle della rilevazione del Data Breach, sono state adottate misure per impedire il concretizzarsi dei rischi per i diritti e le libertà degli Interessati;
- ✓ la notifica del Data Breach a tutti gli Interessati singolarmente comporta uno sforzo sproporzionato rispetto al rischio. In tal caso occorrerà comunque procedere a una comunicazione pubblica o a una misura simile, tramite la quale gli Interessati siano comunque informati con analoga efficacia.

Il Dirigente Scolastico, di concerto con il DPO, valuta di volta in volta, sulla base della tipologia e del numero di Interessati, il canale di comunicazione che appare più opportuno per trasmettere la notifica agli stessi.

In ogni caso la notifica agli Interessati deve contenere quanto meno:

- ✓ nome e dati di contatto del DPO;
- ✓ descrizione delle probabili conseguenze della violazione;
- ✓ descrizione delle misure adottate o che l'Istituto intende adottare per porre rimedio alla violazione e ridurre gli effetti negativi.

Data Breach relativo a dati personali trattati in qualità di Responsabile del trattamento

Qualora, a seguito di una segnalazione o nel corso dell'analisi preliminare di cui al precedente paragrafo, il Dirigente Scolastico rilevasse che la violazione

qualificabile come Data Breach riguarda dati personali di titolarità di un soggetto terzo trattati dall'istituto in qualità di Responsabile del trattamento, procede a informare senza ingiustificato ritardo il soggetto terzo titolare del trattamento.

Nel dettaglio, la comunicazione al soggetto titolare del trattamento dovrà contenere quanto meno le seguenti informazioni (oltre a quelle eventualmente richieste dallo stesso soggetto terzo titolare del trattamento):

- ✓ Descrizione della natura della violazione dei dati personali comprensiva, ove possibile, di informazioni in merito alle categorie e al numero di Interessati nonché alle categorie e al volume approssimativo di dati personali oggetto di violazione;
- ✓ Nome e dati di contatto del DPO;
- ✓ Descrizione delle possibili conseguenze della violazione;
- ✓ Descrizione di eventuali misure già adottate o di cui si prevede l'adozione per porre rimedio alla violazione di dati personali e per attenuarne i possibili effetti negativi.

La comunicazione, nel testo convalidato dal DPO, sarà inviata al soggetto titolare del trattamento entro 48 ore dall'avvenuta rilevazione della violazione o nel minore termine eventualmente indicato dal soggetto titolare del trattamento.

Prescrizioni per la prevenzione di Data Breach

L'Istituto adotta specifiche strategie per prevenire o minimizzare il verificarsi di Data Breach.

In primo luogo, occorre che tutti gli Incaricati Autorizzati al Trattamento siano consapevoli dei Dati personali che trattano attraverso i propri strumenti (anche cartacei) e dispositivi o a cui hanno accesso tramite i sistemi del Titolare del trattamento. A tal fine, la presente procedura viene loro comunicata dal Titolare del trattamento. Essi dovranno custodire tali Dati personali ed i relativi documenti con cura e in modo responsabile sia all'interno che all'esterno della propria area di lavoro. Si precisa che i soggetti in questione sono già stati istruiti per mezzo di nomina ad Incaricati Autorizzati al trattamento e devono attenersi alle prescrizioni impartite.

ALLEGATO 1

Intestazione dell'Istituto

REGISTRO INCIDENTI INFORMATICI

Numero Incidente	**2020/0001**

A. Rilevazione dell'incidente

Data e ora dell'incidente	
Chi ha rilevato per primo l'incidente? Nominativo e riferimenti	
Data e ora di avvio della gestione dell'incidente	
Note e/o breve descrizione dell'incidente	

B. Descrizione dell’incidente

Origine dell’incidente (interna o esterna). Dettagliare bene l’origine	
Sistemi e/o Applicazioni interessati dall’incidente	
Causa dell’incidente (se più cause indicare la prevalente)	
Stato attuale (situazione diagnosticata)	
Tempi previsti per la soluzione	
Note	

C. Caratterizzazione dell'incidente	

Tipo Incidente (virus, attacco, alterazione dati, guasto apparati, sottrazione informazioni, blocchi, malfunzionamenti, ecc.)	
Sistemi colpiti e/o applicazioni colpite	
Funzioni aziendali colpite	
L'entità dell'incidente è tale da farlo rientrare nell'attenzione GDPR? SI/NO	
Numero Clienti/Utenti oppure Numero Dipendenti colpiti dall'incidente (perdita e/o alterazione dati), ecc..	
Tipologia di dati coinvolti	

Tipologia di soggetti coinvolti	
Note	

D. Risoluzione dell'incidente

Misure tampone intraprese nell'immediato	
Ulteriori misure pianificate per la chiusura dell'incidente o poste in essere per evitare il ripetersi dell'incidente	
Sono state allertate le strutture deputate ad attivare le eventuali comunicazioni GDPR? SI/NO	
Se SI, quando? (Data e Ora)	
Se NO, spiegare le motivazioni di mancata comunicazione	
Chiusura incidente (Data e Ora)	

Note	

ALLEGATO 2

COMUNICAZIONE DI DATA BREACH AL GARANTE PRIVACY

1. Titolare del trattamento

Ragione sociale/Nome e Cognome: _____

C.F./P.IVA: _____

Stato: _____

CAP: _____ Città: _____ Provincia: _____

Telefono: _____

Email: _____

PEC: _____

2. Responsabile della protezione dei dati (o nel caso in cui non sia presente il RPD, i riferimenti di un altro soggetto presso cui ottenere più informazioni)

Denominazione: _____

Telefono: _____

Cellulare: _____

Email: _____

PEC: _____

3. Quando si è verificata la violazione di dati personali?

   - ☐ Il _____
   - ☐ Tra il _____ e il _____
   - ☐ In un tempo non ancora determinato
   - ☐ È possibile che sia ancora in corso

4. Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

5. Modalità di esposizione al rischio

Tipo di violazione

- Lettura (presumibilmente i dati non sono stati copiati);
- Copia (i dati sono ancora presenti sul sistema del titolare);
- Alterazione (i dati sono presenti sui sistemi ma sono stati alterati);
- Cancellazione (i dati non sono più sui sistemi del titolare 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 (specificare).

6. Dispositivo oggetto della violazione

- Computer;
- Rete;
- Dispositivo mobile;
- File o parte di un file;
- Strumento di backup;
- Documento cartaceo;
- Altro (specificare).

7. Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione

8. Quali sono le possibili conseguenze derivanti dalla violazione?

9. Indicare le categorie di interessati colpiti dalla violazione

10. Quante persone sono state colpite dalla violazione dei dati personali?

- n. _____ persone;
- circa _____ persone;
- un numero ancora sconosciuto di persone.

11. Numerosità dei dati di cui si presume la violazione

_____

12. Che tipo di dati sono oggetto di violazione?

- Dati anagrafici;
- Indirizzo di posta elettronica;
- Numero di telefono;
- Dati di accesso e di identificazione (user name, password, customer ID, altro);
- Dati relativi a minori;
- Dati particolari di cui all'art. 9 Reg. UE 2016/679;
- Dati giudiziari;
- Copia per immagine su supporto informatico di documenti analogici;
- Ancora sconosciuto;
- Altro (specificare).

13. Livello di gravità della violazione dei dati personali (secondo la valutazione del titolare)

- Basso/trascurabile;
- Medio;
- Alto;
- Molto alto.

14. Misure tecniche e organizzative applicate ai dati oggetto di violazione

15. La violazione è stata comunicata anche agli interessati?

□ Si, è stata comunicata in data _____;

□ No, perché _____.

16. Qual è il contenuto della comunicazione resa agli interessati?

17. Quale canale è stato utilizzato per la comunicazione agli interessati?

18. La violazione coinvolge interessati che si trovano in altri Paesi UE?

□ Si;

□ No.

19. La comunicazione è stata effettuata alle competenti autorità di altri Paesi UE?

□ Si (specificare quali);

□ No.

20. Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione di dati e prevenire simili violazioni future?

Il Titolare del Trattamento

Dirigente Scolastico