POLICY

DATA BREACH

COD. C.07

CONTIENE:

1. **POLICY**

PREMESSA

Un data breach consiste in una violazione della sicurezza che comporta – accidentalmente o illegalmente – la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali, trasmessi, archiviati o altrimenti elaborati. Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità dei dati personali.

- **Perdita di riservatezza**: quando un soggetto terzo accede o riceve dati a lui non destinati (esempi: accesso di hacker al server della scuola; invio di una mail ai genitori contenente dati sensibili di alcuni ragazzi).
- **Perdita di integrità**: quando un evento pregiudica l'integrità dei database (esempi: allagamento degli archivi, incendio in sala server).
- **Perdita di disponibilità**: quando a causa di un particolare evento è impedito al titolare di accedere ai dati (esempi: malware che rende inaccessibili le icone sul desktop).

È a tal riguardo importante evidenziare che il data breach può riguardare tanto i dati contenuti in supporto **cartaceo** che quelli contenuti in un supporto **digitale**. Tutti i data breach sono incidenti di sicurezza, ma non tutti gli incidenti di sicurezza sono necessariamente data breach.
La procedura di gestione del data breach non prevede che l'incaricato comunichi la violazione ad altri soggetti che non siano specificamente il Dirigente scolastico e il DPO (i.e. la Polizia postale). La procedura di gestione del data breach con notifica al Dirigente scolastico e al DPO deve sempre essere effettuata.

TIPOLOGIE RICORRENTI DI DATA BREACH

Alcuni casi tipici di violazione dei dati sono elencati di seguito:

- Furto delle credenziali di autenticazione ed utilizzo delle stesse
- Smarrimento di una chiavetta USB o di un cellulare o laptop con conseguente perdita di documenti contenenti dati personali
- Cancellazione accidentale
- Pubblicazione su internet di graduatorie contenenti dati sensibili
- Invio di dati sensibili a genitori

- Furto di documenti cartacei contenenti dati sensibili
- Accesso a informazioni riservate da parte di utenti non autorizzati

COME GESTIRE UN DATA BREACH. I PRIMI 10 MINUTI.

NOTA BENE: In caso di violazione dei dati, il Titolare ha un massimo di 72 ore per segnalare il problema al Garante.

In caso di incidente di sicurezza (verificato o sospetto), il dipendente/collaboratore della scuola dovrà procedere come segue:

1. Arresta la perdita di dati aggiuntiva: se si tratta di un data breach che coinvolge i sistemi elettronici, porta offline le macchine interessate, ma non spegnerle. Spegni il Wi-Fi o scollega il cavo ethernet dal laptop.
2. Chiamare immediatamente il DPO e il Dirigente scolastico.
3. Registrare il momento della scoperta: inviare una mail a rpd@euservice.it con le seguenti informazioni: chi ha scoperto la violazione, chi l'ha segnalata, a chi è stata segnalata, chi altro ne è a conoscenza e che tipo di violazione si è verificata.

È importante sottolineare che segnalare l'incidente al Dirigente scolastico e al DPO non deve costituire motivo di discriminazione dell'operato del personale ma è anzi il presupposto per il miglioramento della gestione dei dati dell'organizzazione. Più incidenti verranno registrati all'interno del registro delle violazioni, più potranno essere fatte delle formazioni puntuali e contestualizzate da parte del DPO e quindi più l'organizzazione migliorerà la gestione della privacy. La legge chiede al Titolare di notificare la violazione all'Autorità Garante entro 72 ore dall'accaduto; tuttavia, qualora l'incaricato al trattamento si rendesse conto di aver causato un data breach successivamente alle 72 ore ne dovrà dare comunicazione al Dirigente scolastico e al DPO non appena possibile. Infatti, è sempre meglio notificare la violazione, se dovuto, che non farlo perché una violazione scoperta *ex post* dall'Autorità potrà aggravare l'ammontare di eventuali sanzioni.

COME GESTIRE UN DATA BREACH. I SUCCESSIVI 10 MINUTI

Il soggetto (o i soggetti) che hanno scoperto la violazione dei dati devono scrivere un report al DPO contenente le seguenti informazioni:

- il database (anche cartacei) interessati, nonché la causa e l'entità;
- le categorie e il numero approssimativo delle persone interessate
- le categorie e il volume approssimativo dei dati personali interessati
- una descrizione delle possibili conseguenze della violazione dei dati personali
- possibilmente indicare se la violazione è partita dall'interno o dall'esterno della scuola

UNA E-MAIL CON LE SUDDETTE INFORMAZIONI DEVE ESSERE INVIATA IMMEDIATAMENTE AL DPO ALL'INDIRIZZO: rpd@euservice.it

NOTIFICA DI VIOLAZIONE

Il DPO valuterà, dopo aver effettuato l'analisi dei rischi, se si dovrà notificare l'Autorità Garante poiché le violazioni che **non presentano rischi per gli interessati** non dovranno essere notificate all'Autorità. In caso di comunicazione all'Autorità Garante bisognerà compilare apposito modulo presente sul sito dell'Autorità. Il modulo sarà compilato dal Dirigente scolastico, su consiglio del DPO, e trasmesso all'Autorità Garante da parte del Titolare del Trattamento entro un massimo di 72 ore. Se la notifica viene inviata dopo 72 ore, è necessario descrivere il motivo del ritardo. **Attenzione, le 72 ore non conoscono motivi di sospensione, continuando a decorrere anche in giorni quali Natale, Pasqua ed altre festività**. Per questo è necessario comunicare eventuali data breach al DPO anche se a ridosso di giorni solitamente non lavorativi. La

notifica di data breach si effettua tramite apposito portale sul sito del Garante Privacy e raggiungibile al seguente indirizzo: https://servizi.gpdp.it/databreach/s/

La notifica dovrebbe contenere:

1. Una descrizione della natura della violazione dei dati personali, tra cui, se possibile:

- Le categorie e il numero approssimativo delle persone interessate
- Le categorie e il volume approssimativo dei dati personali interessati

2. Il nome e i dettagli di contatto del DPO o di una persona di contatto competente a fornire informazioni
3. Una descrizione delle possibili conseguenze della violazione dei dati personali
4. Una descrizione delle misure adottate o proposte per porre rimedio alla violazione dei dati personali, comprese, se del caso, le misure adottate per mitigare eventuali effetti negativi
5. Una descrizione dei motivi del ritardo se la notifica è stata effettuata dopo il limite di 72 ore.

Se è probabile che la violazione comporti un rischio elevato per la privacy o la sicurezza di un interessato, tali soggetti saranno informati entro 72 ore dalla scoperta della violazione. Per notificare un individuo colpito da una violazione dei dati personali, la natura della violazione dei dati sarà descritta in un linguaggio chiaro e semplice. Se il data breach è un incidente di tipo informatico bisognerà avvisare anche la Polizia Postale. Sarà necessario, inoltre, un dialogo particolarmente approfondito tra il DPO e l'Amministratore di sistema. Se l'incidente informatico rappresenta un rischio elevato per gli interessati e per la rete in generale sarà necessario contattare anche il CSirt (Computer security incident response team) per ricevere istruzioni in merito alla sua gestione.
Tutte le violazioni dei dati personali, indipendentemente dal ricorrere dell'obbligo o meno di segnalarle, saranno registrate dal DPO in un apposito registro (Registro degli incidenti di violazione dei dati), registrando:

- Chi ha notificato la violazione dei dati e data
- Descrizione della violazione dei dati
- Individuo colpito
- Effetti
- Azioni correttive intraprese e data di scadenza
- Se la violazione è stata notificata o meno al Garante

È bene ricordare che in caso di ispezione l'Autorità Garante potrà chiedere il registro delle violazioni che quindi deve essere compilato adeguatamente. Un registro delle violazioni vuoto o mal compilato potrebbe far generare dei sospetti all'Autorità che alla privacy non venga dato il giusto peso. A tal fine si allega un modello di registro di data breach da utilizzare per annotare le precedenti informazioni.

MODELLO REGISTRO DATA BREACH

DESCRIZIONE EVENTO	DATA E ORA EVENTO	FONTE NOTIZIA	TITOLARE TRATTAMENTO	DATA E ORA NOTIFICA	DOVE RINVENIRE PROVA NOTIFICA	PERCHÉ NON È STATO NOTIFICATO IL DATA BREACH	DATA E ORA DI COMUNICAZIONE AGLI INTERESSATI	CATEGORIA DI DATI OGGETTO DI VIOLAZIONE	CATEGORIA DI INTERESSATI COINVOLTI

Il registro dei data breach, una volta compilato dovrà essere munito di data certa, ad esempio, inviando dalla vostra pec alla vostra pec il documento stesso.