Vargiu Scuola Srl
Via dei Tulipani 7/9 – Assemini (CA) - 09032
Sito: vargiuscuola.it
commerciale@vargiuscuola.it
tel: 070271526, 070271560
partita iva: 03679880926

Alle scuole che ci hanno affidato l'incarico di RPD o a cui forniamo servizi di consulenza normativa

VS_DPO 17/2021 Assemini, 17/2/2021

La gestione dei data breach

Nello svolgimento delle proprie attività qualunque azienda o amministrazione pubblica ha a che fare con una grande quantità di dati personali che possono anche essere di natura particolare (i vecchi dati sensibili della normativa privacy) e riguardare lo stato di salute, il credo religioso, le convinzioni politiche o altre informazioni che sono tutelate in maniera più stringente dalla normativa.
Il trattamento dei dati personali deve avvenire nel rispetto dei diritti e dei principi stabiliti dal Regolamento UE (GDPR) e, in base al principio di accountability, spetta al titolare del trattamento **l'onere di adottare misure tecnico/organizzative atte a minimizzare la probabilità di violazione degli stessi dati (personal data breach).**
La prima cosa da chiarire è che i data breach sono connaturati con il trattamento dei dati personali e nessuna misura tecnico/organizzativa può azzerare la probabilità di un incidente. Il titolare è quindi tenuto a mettere in atto un **processo di gestione del data breach** che gli consenta di rendere minimo l'impatto sugli interessati dovuto ad una compromissione dei dati personali, ottemperando nel contempo agli obblighi normativi previsti dallo stesso GDPR e da altre normative di settore.

1. Cosa è il data breach

All'articolo 4, punto 12, il regolamento definisce il **data breach** come *"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"*.

- **Distruzione:** il significato di "distruzione" dei dati personali dovrebbe essere abbastanza chiaro: si ha distruzione dei dati quando gli stessi non esistono più o non esistono più in una forma che sia di qualche utilità per il titolare del trattamento.
- **Perdita:** Con "perdita" dei dati personali si dovrebbe invece intendere il caso in cui i dati potrebbero comunque esistere, ma il titolare del trattamento potrebbe averne perso il controllo o l'accesso, oppure non averli più in possesso.
- **Divulgazione o accesso:** un trattamento non autorizzato o illecito può includere la divulgazione di dati personali a (o l'accesso da parte di) destinatari non autorizzati a ricevere (o ad accedere a) i dati oppure qualsiasi altra forma di trattamento in violazione del regolamento.
- **Modifica:** si verifica un danno quando i dati personali sono stati modificati, corrotti o non sono più completi.

Le violazioni possono essere classificate in base ai seguenti tre principi ben noti della sicurezza delle informazioni:

- ***"violazione della riservatezza"***, in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;

- ***"violazione dell'integrità"***, in caso di modifica non autorizzata o accidentale dei dati personali;
- ***"violazione della disponibilità"***, in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

Va osservato che, a seconda dei casi, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse. Esempi di perdita di disponibilità possono aversi quando i dati vengono cancellati accidentalmente o da una persona non autorizzata, oppure, in caso di dati crittografati in maniera sicura, quando la chiave di decifratura viene persa. Se il titolare del trattamento non è in grado di ripristinare l'accesso ai dati, ad esempio ricorrendo a un backup, la perdita di disponibilità sarà considerata permanente.
Può verificarsi perdita di disponibilità anche in caso di interruzione significativa del servizio abituale di un'organizzazione, ad esempio un'interruzione di corrente o attacco da "blocco di servizio" (*denial of service*) che rende i dati personali indisponibili.

Alcuni esempi di data breach sono:

- sottrazione o copia non autorizzata di un documento cartaceo od informatico contenente dati personali
- perdita o furto di una pen drive, di un notebook o di qualunque altro dispositivo contenente dati personali
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- dati e documenti criptati da un *ransomware* (*malware* del riscatto)
- dati e documenti criptati dal titolare del trattamento mediante una chiave non più in suo possesso
- 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
- Una e-mail che viene inviata ai destinatari nei campi "a:" o "cc:", consentendo così a ciascun destinatario di vedere l'indirizzo e- mail di altri destinatari
- Le cartelle cliniche di un ospedale sono indisponibili per un periodo di 30 ore a causa di un attacco informatico

2. Misure tecniche ed organizzative per minimizzare i data breach

La prima responsabilità del titolare è quella **di adottare misure tecnico/organizzative atte a minimizzare la probabilità di violazione degli stessi dati.** Queste misure devono essere commisurate all'organizzazione ed alla tipologia di dati trattati con rilevanti differenze fra le misure che, ad esempio, deve adottare una scuola e quelle di una azienda sanitaria od una banca.
Gli istituti scolastici, come qualunque pubblica amministrazione, devono comunque garantire le misure di sicurezza ICT definite da **AGID nella *circolare 18 aprile 2017 n°2*** e dichiarate in modo puntuale in un documento da tenere agli atti. VargiuScuola mette a disposizione la bozza di una dichiarazione delle misure di sicurezza ICT adottate dalla scuola e delle modalità con cui esse sono implementate secondo le metodologie e gli strumenti indicati nell'Allegato 1 della circolare AGID. Il documento può essere personalizzato da ciascun istituto anche tramite il coinvolgimento del proprio amministratore di sistema.
Ricordiamo che la gestione della sicurezza passa non solo per l'adozione di misure tecniche ma anche per idonee misure organizzative e per la formazione del personale. E' quindi importante che la scuola definisca e renda noti al personale le istruzioni e le norme di comportamento per lo svolgimento dell'attività lavorativa (vedere, ad esempio, la bozza VargiuScuola delle istruzioni per il personale in smart working).

3. Cosa fare per gestire un data breach

Nessuna misura tecnica o organizzativa potrà mai azzerare la probabilità di una violazione di dati personali (soprattutto in un ambiente scolastico) per cui il titolare ha la responsabilità di predisporre un **processo di gestione del data breach** che gli consenta di minimizzare le conseguenze di un qualunque incidente che coinvolga i dati personali trattati. Anche il processo di gestione del data breach, come prima le misure di sicurezza tecnico/organizzative da adottare, deve essere coerente e compatibile con i dati personali e il tipo di trattamento operato come anche con il contesto ambientale. Con ciò vogliamo dire che il processo di gestione del data breach in un ambiente scolastico non può essere troppo complesso e con troppi livelli di responsabilità e solo in pochi casi fortunati può contare su adeguate competenze interne.

Per la gestione dei data breach suggeriamo prima di tutto di **produrre delle specifiche linee guida** che definiscano cosa fare in occasione di una violazione di dati personali (vedere la bozza VargiuScuola per le scuole in contratto).

E' poi necessario informare tutto il personale su cosa sia una violazione di dati personali e sulle procedure adottate dalla scuola per la sua gestione. Suggeriamo quindi di formalizzare una **circolare contenente istruzioni specifiche al personale** nel caso in cui riconoscano un data breach nello svolgimento delle proprie attività lavorative (questo il link alla bozza VargiuScuola).

Altro tassello fondamentale per la gestione dei data breach è la **formazione**. Allo scopo di fornire istruzioni ed informazioni utili VargiuScuola ha realizzato uno specifico wiki sulla gestione dei data breach.

4. Cosa fare se si viene a conoscenza di un data breach

Nella circolare tutto il personale deve essere informato dell'obbligo di comunicare tempestivamente al dirigente scolastico qualunque violazione di dati personali di cui dovesse venire a conoscenza. In caso di emergenza e di temporanea indisponibilità del dirigente scolastico il personale può essere autorizzato a contattare direttamente il responsabile protezione dati (RPD), l'Amministratore di Sistema o altre eventuali figure, interne od esterne, che gestiscono i sistemi informatici e la sicurezza dei dati. Nella circolare è opportuno riportare quindi i dati di contatto delle figure deputate a gestire il data breach (nella circolare indicare se VargiuScuola è per il vostro istituto RPD o amministratore di sistema).

5. La gestione del data breach

Dopo il primo immediato intervento volto a contenere l'entità del data breach e a limitare i danni è necessario che il dirigente scolastico, di concerto con l'RPD ed altre eventuali figure tecniche o consulenziali di cui si avvale la scuola per la gestione della privacy e dei sistemi informatici, provveda ad effettuare una indagine più approfondita volta a definire la gravità della violazione. In questa fase bisognerà identificare i possibili rischi derivanti dalla violazione e definire le azioni da intraprendere per la loro minimizzazione. In questa fase il dirigente scolastico dovrà valutare l'opportunità o la necessità di fare la comunicazione al Garante, che dovrà intervenire entro le 72 ore dalla conoscenza del fatto, ed eventualmente alle persone fisiche minacciate nei loro diritti dall'evento. In merito alla scelta dovranno essere coinvolti ed esprimeranno il proprio parere il RPD ed eventuali altri consulenti informatico/normativi ma la decisione finale dovrà essere del dirigente scolastico che sarà responsabile in base al principio della responsabilizzazione.

Nel momento in cui il titolare del trattamento dovesse decidere in modo difforme dal parere espresso dal RPD è opportuno che rediga un documento per illustrare le motivazioni che l'hanno indotto alla scelta.

Ricordiamo che l'art. 33 del Regolamento Europeo 679/2016 (GDPR) impone al titolare del trattamento di notificare all'autorità di controllo (Garante privacy) la violazione di dati

personali **entro 72 ore dal momento in cui ne viene a conoscenza**. L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche, qualora, poi, il rischio fosse elevato, allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all'interessato.

6. La notifica al Garante

A partire dal 1° luglio 2021, la notifica di una violazione di dati personali deve essere inviata al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/ (VEDI: Provvedimento del 27 maggio 2021). Nella stessa pagina è disponibile un modello facsimile, da NON utilizzare per la notifica al Garante ma utile per vedere in anteprima i contenuti che andranno comunicati al Garante. All'indirizzo https://servizi.gpdp.it/databreach/s/istruzioni le istruzioni per l'utilizzo della procedura telematica per la notifica delle violazioni dei dati personali.

Per semplificare gli adempimenti previsti per i titolari del trattamento, il Garante ha ideato e messo disposizione un apposito **strumento di autovalutazione (self assessment)** che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza.

7. Il registro delle violazioni

La normativa prevede che tutti i titolari di trattamento devono in ogni caso documentare le violazioni di dati personali subite, **anche se non notificate all'Autorità di controllo e non comunicate agli interessati**, nonché le relative circostanze e conseguenze e i provvedimenti adottati (art. 33, paragrafo 5, GDPR). Ciò significa che la scuola deve tenere costantemente aggiornato un **registro delle violazioni** che, per semplicità di gestione, abbiamo deciso di integrare nel registro dei trattamenti la cui bozza Vargiu Scuola è scaricabile dal presente link. Rileviamo che la registrazione del data breach è importante anche nel caso in cui non sia fatta la comunicazione al Garante anche perchè, in caso di contestazione della omessa notifica non si aggiunga ad essa l'aggravante della omessa annotazione nel registro delle violazioni, fatto che potrebbe far pensare ad una volontà di tenere nascosto l'evento e che potrebbe avere un peso rilevante nella valutazione dell'entità di una eventuale sanzione.

E' peraltro evidente che la comunicazione al Garante può essere fatta con una certa serenità solo se la scuola ha adempiuto almeno agli obblighi formali relativi alle nomine e alla predisposizione dei documenti previsti dalla normativa e che potrebbero essere oggetto di verifica da parte dell'autorità di controllo.

E se non l'RPD non è stato nominato?
Poiché non sempre le scuole sono solerti nel garantire la formalizzazione della nomina del RPD mettiamo in evidenza quale sia la difficolta in cui si potrebbe trovare il dirigente che dovendo fare la comunicazione di un data breach al Garante entro 72 ore dal momento in cui è venuto a conoscenza della violazione, non è in grado di indicare nella comunicazione i riferimenti del proprio RPD perché non nominato. In tal caso la notifica del data breach al Garante equivarrebbe ad un auto-denuncia dell'omessa nomina del RPD. La scelta di omettere la notifica è peraltro ad alto rischio perché nel momento in cui il Garante fosse coinvolto da terzi (ad esempio le vittime del data breach che fanno una segnalazione) il dirigente dovrebbe rispondere sia della omessa nomina del RPD che della omessa notifica del data breach al Garante.