INFORMAZIONI CIOFS E CNOS/SCUOLA
30/2021
A cura di d. Bruno Bordignon

930/21 Attacco informatico e Data Breach a scuola: valutazione delle violazioni di dati o sistemi. Scarica il documento da utilizzare per la procedura

di *Antonio Fundarò*

Lo scopo di questa procedura è quello di definire gli elementi che caratterizzano una violazione di dati personali al fine di: riconoscere una violazione; valutare le conseguenze; valutare gli adempimenti derivanti; o comunicazione al garante o comunicazione agli interessati; valutare le misure di sicurezza da correggere o adottare.

La valutazione, da parte del Dirigente scolastico

La valutazione, da parte del Dirigente scolastico, deve essere effettuata rapidamente, prevedibilmente entro 72 ore dalla sua consapevolezza.
Se la violazione – come si legge nel Data Breach dell'Istituto comprensivo est 1 di Brescia, diretto con grande competenza e professionalità eccellente dal dirigente scolastico prof. Gaetano Greco – avviene sui sistemi affidati ad un responsabile, questi ne informa il Titolare "senza ingiustificato ritardo". Da quel momento, e non dal verificarsi della violazione, decorreranno le 72 ore per la valutazione e la eventuale segnalazione.

Riconoscere che si è verificata una violazione

È quindi necessario riconoscere innanzitutto che si è verificata una violazione:

- la violazione di sicurezza che comporta accidentalmente o in modo illecito
- la distruzione
- la perdita
- la modifica
- la divulgazione non autorizzata
- l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Il concetto di "perdita"

Il concetto di "perdita" necessita di un approfondimento.
Secondo il Garante: 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

Riferimenti normativi

Nelle "Linee guida sulla notifica delle violazioni – GDPR" si legge all'articolo 33 Notifica di una violazione dei dati personali all'autorità di controllo: "In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo".

Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo

Il responsabile del trattamento – come si legge nel Data Breach dell'Istituto comprensivo est 1 di Brescia, diretto dal dirigente scolastico prof. Gaetano Greco – informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
La notifica deve:

- descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

Articolo 34: Comunicazione di una violazione dei dati personali all'interessato
Quando la violazione dei dati personali – come si legge nel Data Breach dell'Istituto comprensivo est 1 di Brescia – è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:

- il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

Tipi di violazione
Le violazioni possono esser classificate in base a tre principi:

- "violazione della riservatezza", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzato o accidentale;
- "violazione dell'integrità", in caso di modifica non autorizzata o accidentale dei dati personali;
- "violazione della disponibilità", in caso di perdita, accesso15 o distruzione accidentali o non autorizzati di dati personali.

La valutazione della violazione della disponibilità può avere elementi di indeterminatezza. Una perdita o una distruzione permanenti dei dati saranno sempre considerate violazioni della disponibilità. Tuttavia, come possiamo considerare la indisponibilità temporanea?

Cosa afferma il garante
Afferma il Garante che: nell'attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, si dovrebbe prendere in considerazione, tra le altre cose, "la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento" e "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico".
Di conseguenza, un incidente di sicurezza che determina l'indisponibilità dei dati personali per un certo periodo di tempo costituisce una violazione, in quanto la mancanza di accesso ai dati può avere un impatto significativo sui diritti e sulle libertà delle persone fisiche.

Valutazione dell'impatto
Dunque, anche un evento che ci ha privato temporaneamente della disponibilità dei dati deve comportare una valutazione dell'impatto che può avere avuto sui diritti e sulle libertà delle persone, così come una perdita di disponibilità definitiva, un accesso non autorizzato o la diffusione non controllata.
Risulta quindi fondamentale che il titolare, e in alcuni casi prima di lui il responsabile, ne venga a conoscenza tempestivamente.
Non tutte le violazioni attiveranno la necessità di notificare al Garante o agli interessati, ma senz'altro tutte dovranno essere annotate nei loro elementi salienti così come dovranno essere annotate le valutazioni in base alle quali verranno prese le decisioni successive.

Procedura di valutazione delle violazioni
È possibile suddividere la procedura di valutazione delle violazioni nelle seguenti fasi:

- riconoscimento del sussistere della violazione
- comunicazione degli elementi da valutare
- annotazione sul registro
- valutazione degli elementi
- eventuale notifica al Garante
- eventuale notifica agli interessati
- completamento dell'annotazione sul registro
- eventuale indicazione di nuove misure di sicurezza e loro verifica
- inseriamo il diagramma delle fasi contenuto nel documento WP250.
- **Procedura_databreach**

Attacco informatico e Data Breach a scuola: valutazione delle violazioni di dati o sistemi. Scarica il documento da utilizzare per la procedura - Orizzonte Scuola Notizie