INFORMAZIONI CIOFS E CNOS/SCUOLA
46/2020
A cura di d. Bruno Bordignon

964/20 GDPR, sicurezza del trattamento e data breaches: cosa deve fare la scuola per evitare o gestire le violazioni della sicurezza dei dati

di *Avv. Bruno Cantarone*

Nel passaggio dalla previgente disciplina del Codice della Privacy all'odierno GDPR il ruolo del titolare del trattamento ha acquisito ben maggiore importanza nella concreta strutturazione delle **misure di sicurezza** da apprestare a protezione dei dati personali.
Perduto il rassicurante novero delle misure "minime" da adottare in caso di trattamento con strumenti elettronici, quelle previste dal Disciplinare Tecnico meglio noto come "Allegato B" al Codice della Privacy (abrogato dall'articolo 27, comma 1, lett. d), del decreto legislativo 10 agosto 2018, n. 101), il titolare del trattamento è infatti oggi chiamato ad effettuare una analisi risk based per decidere, all'atto pratico, gli interventi necessari.
Il balzo in avanti è di notevole entità, in quanto gli si chiede di dimenticare – nella gestione della protezione dei dati – quell'approccio metodologico burocratico-prescrittivo che prima lo vincolava ad impiegare, nel minimo, talune misure predeterminate (quelle contenute nel citato "Allegato B"), per assumere ora – in ottica di accountability,ai sensi dell'art. 24 – un approccio manageriale basato appunto sul rischio, che lo impegna a mettere in atto misure tecniche ed organizzative (non più minime bensì) adeguate.
In definitiva il titolare deve determinare, in base ad una valutazione oggettiva, la probabilità e la gravità del rischio per i diritti e le libertà dell'interessato, avendo riguardo alla natura, all'oggetto, al contesto ed alle finalità del trattamento, per giungere a stabilire quali misure tecniche ed organizzative risultino adeguate nel caso specifico, tenuto altresì conto dello stato dell'arte e dei costi della loro eventuale attuazione.
Nella scelta di queste misure (che andranno poi inserite nell'obbligatorio Registro delle attività di trattamento, ai sensi dell'art. 30, lett. g), il titolare, dati i diversi fattori in gioco e le numerose variabili che possono influenzare le sue valutazioni, gode, almeno in astratto, di una certa discrezionalità.
Il GDPR non fornisce infatti all'interprete un catalogo completo di misure adeguate, limitandosi a segnalarne solo alcune (art. 32, par. 1), come la pseudonimizzazione e la cifratura dei dati (lett. a) – tecniche che nell'intero corpo del medesimo Regolamento Ue 2016/679 vengono più volte richiamate quali tecniche ideali per aumentare la protezione dei dati, soprattutto di quelli sensibili – o come la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento (lett. b), la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico (lett. c), o ancora, come l'implementazione di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure attivate al fine di garantire la sicurezza del trattamento.
Corrispondentemente, un inizio di catalogo è anche quello che riguarda i possibili rischi cui possono essere esposti i dati personali durante il trattamento, rischi che l'art. 32, par. 2, così individua: distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, ai medesimi dati trasmessi, conservati o comunque trattati.
Si tratta di rischi che mettono in vario modo in pericolo quella che viene definita la "triade della sicurezza informatica" (cyber security) ossia i tre pilastri sui quali impostare la corretta gestione e protezione dei dati: confidenzialità, integrità e disponibilità.
L'avverarsi di uno qualunque dei rischi sopra elencati configura una violazione dei dati personali (data breach) le cui cause sono in genere riconducibili alle tre macro aree qui di seguito riportate,

con i relativi esempi, sulla scorta di una 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: 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).

L'ampiezza dello spettro di cause potenzialmente in grado di minare la cd. triade della cybersecurity esponendo a rischio i dati trattati dovrebbe, di per sé, indurre ogni titolare a prepararsi a gestire le conseguenze delle eventuali violazioni della sicurezza che, nonostante tutti i suoi sforzi per impedirne l'insorgere, possono comunque verificarsi.

Un evento qualificabile come data breach fa infatti scattare tre adempimenti (in linea di principio) obbligatori: 1) notifica della violazione al Garante; 2) comunicazione della violazione all'interessato; 3) istituzione di un registro che documenti l'avvenuta violazione, indicandone le circostanze, le conseguenze ed i provvedimenti assunti per porvi rimedio.

A parte quest'ultimo adempimento, è opportuno che gli altri due vengano convenientemente valutati da parte del titolare del trattamento con l'assistenza del Responsabile della protezione dei dati, in quanto gli articoli 33 e 34 del GDPR prevedono che, ricorrendo specifiche circostanze, sia la notifica della violazione che la comunicazione all'interessato possano essere legittimamente omesse.

Per quanto riguarda la notificazione al Garante l'art. 33 pone in capo al titolare del trattamento, non appena viene a conoscenza dell'avvenuta violazione, un generale obbligo di notifica che deve aver luogo senza ingiustificato ritardo e, se possibile, entro 72 ore (decorso tale termine, la notifica della violazione deve essere corredata delle ragioni del ritardo).

Attraverso tale notifica all'autorità garante il titolare: a) descrive la natura della violazione dei dati personali, compresi, ove possibile, le categorie e il numero approssimativo di interessati; b) comunica il nome e i dati di contatto del Responsabile della protezione dei dati; c) descrive le probabili conseguenze della violazione dei dati personali; d) descrive le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e per mitigarne i possibili effetti negativi.

Tale obbligo però non sorge se il titolare – compiute le necessarie verifiche – è in grado di dimostrare che è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Detto in altri termini, la notifica dell'avvenuta violazione non è strettamente obbligatoria, essendo subordinata, come peraltro ha sottolineato lo stesso Garante italiano, alla valutazione che il titolare deve svolgere in ordine all'effettivo rischio per gli interessati.

Similmente è a dirsi per quanto riguarda la comunicazione all'interessato, comunicazione che nonostante l'avvenuta violazione della sicurezza dei dati, non è richiesta se è soddisfatta almeno una delle condizioni che l'art. 34 annovera al paragrafo 3: a) 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; b) 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 cui appartenevano i dati violati; c) la comunicazione comporterebbe sforzi sproporzionati (in tale evenienza si procede invece a una comunicazione

pubblica o a una misura simile, tramite la quale gli interessati vengono informati con analoga efficacia).
Anche in questo caso, l'adempimento può quindi risultare – in esito ad un attento discernimento condotto a lume delle indicazioni fornite dalla norma di riferimento – del tutto evitabile senza minimamente intaccare la compliance.
E' auspicabile pertanto che, sia nella progettazione ed allestimento delle misure di sicurezza atte a scongiurarli, sia nella gestione degli eventi avversi che dovessero verificarsi durante il trattamento, il titolare possa sempre contare sulla competenza e professionalità del Responsabile della protezione dei dati, per operare consapevolmente, anche in questi ambiti, le scelte più appropriate.
Avv. Bruno Cantarone: cassazionista, Privacy Officer, consulente e formatore privacy nonché Responsabile della Protezione dei Dati per numerose istituzioni scolastiche pubbliche di ogni ordine e grado.
GDPR, sicurezza del trattamento e data breaches: cosa deve fare la scuola per evitare o gestire le violazioni della sicurezza dei dati - Orizzonte Scuola Notizie