Vademecum sul *data breach*

Le istituzioni scolastiche, in quanto organizzazioni che trattano dati personali, sono tenute al rispetto del Regolamento Generale sulla protezione dei dati (GDPR) che impone la segnalazione di alcuni tipi di violazione dei dati all'autorità di vigilanza.

Proponiamo, di seguito, una guida operativa per la notifica di un eventuale *data breach.*

Cos'è	Una **violazione di sicurezza** che comporta, colpevolmente o incolpevolmente, **la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali** trasmessi, conservati o comunque trattati **Alcuni esempi:** - l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati - il furto o la perdita di dispositivi informatici contenenti dati personali - la deliberata alterazione di dati personali - l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, come virus, *malware* ecc. - 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
Cosa fare	**Contattare con urgenza il DPO** per iscritto per valutare quali azioni occorre porre in essere: - interventi di minimizzazione della violazione - formazione specifica al personale - rimodulazione delle misure adottate dall'Istituto a tutela della *privacy* - notifica al Garante. Questo adempimento è obbligatorio al ricorrere di "effetti avversi significativi" (v. dopo): la relativa valutazione deve essere compiuta, consultando appunto il DPO
Quando occorre fare una notifica al Garante	Devono essere notificate solo le violazioni di dati personali che possono avere **effetti avversi significativi** sugli individui, causando danni fisici, materiali o immateriali. **Alcuni esempi:** - la perdita del controllo sui propri dati personali - il furto d'identità o il rischio di frode - la perdita di riservatezza dei dati personali protetti dal segreto professionale - una perdita finanziaria - un danno alla reputazione
Contenuto della notifica al Garante	La notifica deve contenere le informazioni previste all'art. 33, par. 3 del Regolamento (UE) 2016/679 e indicate nell'allegato al **Provvedimento del Garante del 30 luglio 2019 sulla notifica delle violazioni dei dati personali (doc. web n. 9126951)**
Come inviare la notifica	La notifica, sottoscritta digitalmente, deve essere inviata al Garante: - tramite pec all'indirizzo **protocollo@pec.gpdp.it** oppure - tramite peo, all'indirizzo **protocollo@gpdp.it**. Se trasmessa con firma autografa, la notifica deve essere presentata unitamente alla copia del documento d'identità del firmatario. L'oggetto del messaggio deve contenere obbligatoriamente la dicitura **"NOTIFICA VIOLAZIONE DATI PERSONALI"** e, solo opzionalmente, la denominazione del titolare del trattamento.

	La trasmissione della notifica deve avvenire entro 72 ore dal *data breach*.
Cosa fa il Garante	Il Garante può: - **prescrivere misure correttive** nel caso sia rilevata una violazione delle disposizioni del Regolamento stesso, anche per quanto riguarda l'adeguatezza delle misure di sicurezza tecniche e organizzative applicate ai dati oggetto di violazione - **comminare sanzioni pecuniarie**

Fonte: *https://www.garanteprivacy.it/regolamentoue/databreach*

Conclusioni

Alla luce della delicatezza dei dati trattati dalle Istituzioni scolastiche e **tenendo conto del fatto che un'eventuale sanzione pecuniaria sarà a carico del dirigente scolastico**, si consiglia di:

- fornire formale incarico al trattamento dei dati al personale dipendente (secondo il Garante della *privacy*, infatti, "si ritiene che titolari e responsabili del trattamento possano mantenere in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento così come delineatesi negli anni anche attraverso gli interventi del Garante in quanto misure atte a garantire e dimostrare "che il trattamento è effettuato conformemente" al regolamento")
- formare periodicamente il personale dipendente circa gli adempimenti prescritti a tutela della *privacy*
- contattare il DPO tempestivamente in caso si verifichi una fattispecie astrattamente riconducibile al *data breach*.