PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 24 - numero 5130 di Venerdì 25 marzo 2022

GDPR: un apprezzabile esempio di come si devono applicare le sanzioni

Ringrazio a nome dei lettori l'autorità garante britannica, Information Commissioner Office, per aver applicato una doverosa sanzione ad un titolare, in piena conformità alle indicazioni del regolamento generale europeo.

Allego a questa notizia un documento, pubblicato dall'autorità garante britannica-ICO, che ha ritenuto appropriato applicare una sanzione ad un titolare del trattamento, che già era stato abbondantemente penalizzato dall'aver dovuto pagare un riscatto, per un attacco per ransomware.

Il documento allegato è quanto mai apprezzabile, in quanto esso illustra, punto per punto, secondo i dettati del regolamento generale europeo, le modalità di valutazione di una infrazione al regolamento e le modalità di calcolo di una sanzione.

Ricordo ai lettori che tutte le sanzioni, in materia di violazione del regolamento europeo, devono essere valutate sulla base dell'analisi puntuale di ben 11 aspetti della violazione stessa, inclusi alcuni aspetti particolari.

Un documento che giunge all'applicazione della sanzione, dopo una analisi acribica di tutti gli aspetti afferenti alla violazione, è un documento che prova, al di là di ogni dubbio, l'approccio corretto dell'autorità garante, rispetto all'approccio, adottato da altre autorità garanti, che non analizzano puntualmente ogni singolo aspetto della violazione.

Questo documento risulta poi particolarmente interessante in quanto la sanzione viene applicata ad uno studio legale, che già aveva dovuto pagare una somma non precisata per riscattare i dati personali dei clienti, che erano stati cifrati da un attacco per ransomware.

A Roma c'è un'espressione abbastanza colorita, ma chiarissima, che si applica proprio una situazione del genere!

Il motivo per cui è stata applicata la sanzione è legato al fatto che l'attacco per ransomware è stato perpetrato da ignoti, sfruttando delle debolezze del sistema informativo del titolare attaccato, che erano già ben note al titolare ed alle quali egli stava

ponendo rimedio con un certo lassismo.

L'autorità garante britannica ha ricordato che esiste comunque un obbligo, in capo ogni titolare, di proteggere in modo adeguato il sistema di trattamento di dati personali.

Pur comprendendo il fatto che non esiste un sistema perfetto di protezione, l'autorità garante ha messo in evidenza come le debolezze, sfruttate dall'attaccante, erano già ben note al titolare ed egli poco aveva fatto per metterle sotto tempestivo controllo.

Ma ciò che mi ha colpito in modo particolare, nell'esaminare il documento che giunge alla determinazione della sanzione, dopo una analisi puntuale di ogni singolo aspetto, legato alla violazione stessa, deriva proprio dal fatto che l'estensore della sanzione ha preso in esame ogni singolo aspetto, degli 11 previsti dal regolamento, esprimendo un giudizio, sulla base dei quali evidentemente si può giungere, alla fine, alla determinazione della specifica gravità della violazione e quindi della determinazione della sanzione.

Ho già fatto presente in altre circostanze come questo approccio, tenuto ad esempio dal garante islandese, sia l'unico che permetta di effettuare una analisi completa della violazione e, soprattutto, rendere più difficoltoso, da parte del soggetto sanzionato, l'avvio di un potenziale ricorso.

L'applicazione di sanzioni di tipo cumulativo, se non proprio forfettario, non supportata da procedimenti analitici di valutazione dei singoli aspetti della votazione, rappresenta uno degli aspetti più negativi nel comportamento di varie autorità garanti europee.

Mi auguro che questo documento possa costituire una più che corretta base di riferimento per tutte le autorità europee, che debbono applicare sanzioni, rispettando puntualmente l'analisi dettagliata degli 11 parametri previsti dal regolamento europeo.

Vedi allegato

Adalberto Biasiotti

www.puntosicuro.it