PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 4898 di Mercoledì 24 marzo 2021

Come si valuta la gravità di una violazione in materia di protezione dei dati

Una significativa sanzione motivata da una notifica di violazione di dati personali in conformità alle indicazioni del regolamento europeo.

Il regolamento generale europeo prescrive in modo analitico le modalità con cui occorre valutare la gravità di una violazione in materia di protezione dei dati, come premessa per determinare la sanzione. In Romania si è verificata una situazione che merita particolare attenzione.

Ecco i fatti.

L'autorità garante della protezione dei dati della Romania ha affibbiato una significativa sanzione alla Raiffeisen Bank, che opera anche in Italia, e ad una azienda collegata.

La sanzione è motivata da una notifica di violazione di dati personali, avanzata proprio dalla stessa banca, in conformità alle indicazioni del regolamento europeo.

La violazione di sicurezza consisteva nel fatto che due dipendenti della banca, utilizzando i dati estratti dai documenti d'identità di alcuni clienti, che erano stati loro trasmessi da una società collegata, che offriva affidamenti a credito, avevano preso contatto con il Credit Bureau per determinare la affidabilità di questi soggetti, prima dell'affidamento di un credito.

Queste valutazioni preliminari erano state fatte utilizzando un applicativo usato dalla banca per le attività di gestione del credito; la decisione negativa, circa la possibilità di effettuare l'affidamento, era stata comunicata all'azienda collegata, violando procedure interne.

La sanzione è stata imposta al titolare del trattamento perché non aveva attuato le appropriate misure di protezione dei dati, limitando l'accesso ai dati ai soli soggetti autorizzati ed inoltre non aveva attuato adeguate misure tecniche e organizzative, che garantissero un idoneo livello di protezione dei dati.

Una sanzione, di importo assai inferiore, è stata comminata anche l'azienda collegata.

La banca non è rimasta soddisfatta del processo istruttorio sviluppato dall'autorità Garante rumena, in quanto esso non rispecchiava puntualmente l'analisi, articolata in 11 punti, ben illustrata nell'articolo 83 del regolamento generale europeo. Al proposito, vale la pena di sottolineare che in realtà i punti da analizzare sono ben più di 11, perché qualche punto è articolato in sotto punti.

La banca ha pertanto avanzato ricorso alla magistratura ordinaria, che ha ridotto in maniera drammatica la sanzione applicata.

Tra le motivazioni della riduzione della sanzione vi è proprio il fatto che lo svolgimento del processo istruttorio non è stato ritenuto sufficientemente analitico.

Mi permetto di segnalare quanto accaduto ai lettori, perché più volte ho avuto occasione di rilevare come le autorità Garanti europee, in fase di conduzione del processo istruttorio, spesso accorpano in un'unica valutazione elementi, che dovrebbero essere analizzati individualmente; ciò può portare ad una valutazione complessiva non appropriata.

Al proposito, ricordo che una delle autorità Garanti europee da prendere a modello è l'autorità garante islandese, che per ogni processo istruttorio analizza punto per punto tutte le varie lettere, illustrate al comma 1 dell'articolo 83.

È un modello di comportamento che vivamente apprezzo e che sarebbe opportuno fosse attuato da tutte le autorità Garanti europee.

Articolo 83 Condizioni generali per infliggere sanzioni amministrative pecuniarie

1. Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui ai paragrafi 4, 5 e 6 siano in ogni singolo caso effettive, proporzionate e dissuasive.

2. Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle misure di cui all'articolo 58, paragrafo 2, lettere da a) a h) e j), o in luogo di tali misure. Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi:

a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;

b) il carattere doloso o colposo della violazione;

c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;

d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;

e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;

f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

g) le categorie di dati personali interessate dalla violazione;

h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;

i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;

j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; e

k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

Adalberto Biasiotti

www.puntosicuro.it