Formica & Associati

Studio Legale

IL CASO “DATA BREACH” DELL’UNIVERSITA’ CAMPUS BIO-MEDICO DI ROMA E LA VIOLAZIONE DEI DATI PERSONALI DI 74 PAZIENTI

[column width="1/1" last="true" title="" title_type="single" animation="none" implicit="true"] [A cura della Dott.ssa Soraya El Hachimi] **Un importante sviluppo pratico in materia di protezione dei dati personali é stato compiuto con il provvedimento di recente emanato dal Garante Privacy per sanzionare un episodio di c.d. “*data breach*”.**

* * * * *

La vicenda: in data 1 Ottobre 2020 veniva comminata nei confronti dell’Università Campus Bio-medico di Roma una sanzione di euro 20'000,00 (ventimila) per trattamento illecito dei dati in violazione dei principi di liceità, correttezza e trasparenza previsti dall’ art. 5 del Reg. UE/2016/679. Nell’accertare l’avvenuta violazione della specifica disciplina posta a protezione dei dati personali delle persone fisiche, il Garante ha preso in considerazione l’accadimento per cui attraverso il portale del campus Bio-medico un numero limitato di utenti, nell’atto di usufruire del servizio di consultazione online delle immagini e dei referti radiologici, ha potuto visualizzare le informazioni sensibili relative alla salute di altri 74 pazienti-utenti. Un *bug* informatico, dunque, che ha causato una divulgazione indebita di dati personali (c.d. sensibili) la cui visione avrebbe dovuto essere invece riservata ai singoli utenti.

* * * * *

LE RICADUTE NORMATIVE E SANZIONATORIE DEL CASO E LE VALUTAZIONI DEL GARANTE L’art. 33 del Regolamento tipizza l’onere di notifica della violazione all'autorità di controllo, che deve avvenire nel caso in cui il “data breach” — nozione piuttosto ampia che può comprendere una serie variegata di situazioni — presenti un **rischio per i diritti e le libertà di persone fisiche**, e senza ingiustificato ritardo: in ogni caso, entro 72 ore dal momento in cui ne è venuto a conoscenza. Qualora la notifica della violazione all'autorità di controllo non avvenga entro 72 ore, sarà cura del titolare del trattamento illustrare dettagliatamente i motivi del ritardo di tale comunicazione. Nel caso che occupa, dall’attività istruttoria condotta a seguito della segnalazione della violazione all’autorità di controllo, il Garante ha però accertato che, non appena venuto a conoscenza dell’evento, il titolare del trattamento ha **tempestivamente adottato misure correttive** sospendendo il servizio di consultazione online e segnalando l’anomalia di funzionamento al fornitore del sistema informatico. Specificatamente, nell’infliggere la sanzione al Campus Bio-medico di Roma si é tenuto conto sia della “*perdita di riservatezza di una quantità piuttosto limitata di dati personali*” che dell’assenza di download dei documenti sanitari durante gli accessi accidentali. Si é constatata, inoltre, l’assenza di volontarietà nella causazione dell’evento e un elevato grado di collaborazione nella condotta dello stesso. In ragione dei suddetti elementi ed in virtù del limitato pregiudizio inferto, il Garante per la protezione dei dati personali ha ingiunto all'Università Campus Bio-medico di pagare la “modesta” somma di euro ventimila a titolo di sanzione amministrativa pecuniaria. **STRUMENTI DI PREVENZIONE** Il caso dell’Università Campus Bio-medico di Roma dimostra che una certa sollecitudine, la leale cooperazione con l'autorità di controllo, e l'adozione di adeguati modelli organizzativi nella gestione dei dati personali possono premiare il titolare del trattamento (ente, azienda, associazione), oltre che aiutarlo nella pronta individuazione di rischi e violazioni, e nel porvi rimedio (nel caso di specie, segnalando l'accaduto all'Autorità di controllo). Nel caso in oggetto, è necessario che l’ente potenzialmente interessato dal “*data breach*” si doti anche di processi valutativi interni**,** che — in ossequio al principio di *accountability* — gli permettano di giustificare l’eventuale mancata (o il ritardo nella)

segnalazione all'Autorità Garante, perché la violazione non presenterebbe "*un rischio per i diritti e le libertà di persone fisiche*". E' parimenti necessario, qualora la violazione (come in questo caso) derivi da un malfunzionamento del sistema informatico, prevedere presidi contrattuali idonei a meglio allocare e/o mitigare le responsabilità patrimoniali derivanti dalle violazioni, ad es., attraverso patti di manleva o garanzie patrimoniali a carico dell'amministratore di sistema. [/column]