Data breach: l’autodenuncia non esonera il titolare del trattamento dalle proprie responsabilità

Data: 9 gennaio 2020 | Autore: Redazione

Privacy. Data breach: l’autodenuncia tempestiva non esonera il titolare del trattamento dalle proprie responsabilità

Nel provvedimento 141 del 9 luglio 2020 (doc. web n. 9440117) il Garante evidenzia come la tempestività del titolare del trattamento nell’effettuare la notificazione di un data breach e l’immediata adozione di misure correttive non esonerano lo stesso da responsabilità per il trattamento illecito di dati personali.

Il fatto - Un istituto ospedaliero notificava al Garante una violazione dei dati personali sanitari di un paziente.

In particolare, circa una settimana prima della notifica l’istituto aveva ricevuto la segnalazione di un paziente, il quale rappresentava di aver trovato nel proprio fascicolo sanitario elettronico i dati sanitari di un altro paziente.

Dall’istruttoria condotta dal Garante emergeva che l’azienda sanitaria, all’esito delle indagini interne avviate subito dopo aver ricevuto la segnalazione e conclusesi dopo circa 5 giorni, aveva preso contezza della violazione ed aveva effettuato la notifica della violazione all’Authority.

Il Garante, pur tenendo conto del fatto che la notifica era stata eseguita correttamente, ha censurato l'istituto sottolineando che "Il trattamento di dati personali oggetto della comunicazione di "data breach" è stato effettuato in violazione dei richiamati principi di integrità e riservatezza, derivante dall'erronea attribuzione di un referto ad un soggetto diverso dall'interessato, causata da una non corretta applicazione delle misure tecniche e organizzative predisposte dalla Fondazione, al fine di garantire la corretta identificazione dell'interessato" e che "A prescindere dalla notificazione della violazione di dati personali effettuata dal titolare del trattamento in osservanza dell'obbligo di cui all'art. 33 del Regolamento, i profili di illiceità del trattamento rilevati nel caso di specie, quale conseguenza della mancata adozione di misure tecniche e organizzative adeguate, richiedono comunque l'intervento correttivo di questa Autorità al fine di salvaguardare i diritti e le libertà fondamentali degli interessati."

Il Garante ha, quindi, sanzionato l'istituto con l'ammonimento, considerate le circostanze del caso concreto che attenuavano la gravità della violazione (episodio unico e isolato, determinato da un errore umano non intenzionale di un operatore in servizio presso il titolare del trattamento; notifica effettuata dal titolare del trattamento che ha informato dell'accaduto l'interessato e ha adottato molteplici atti organizzativi e iniziative formative volte a sensibilizzare le persone autorizzate al trattamento al rispetto della disciplina in materia di protezione dati personali e al rispetto delle procedure adottate in tema di corretta identificazione dei pazienti).

Considerazioni - Il provvedimento è interessante, in quanto evidenzia ancora una volta come, in caso di data breach che presenti rischi per gli interessati, il titolare del trattamento sia posto di fronte alla scelta tra due opzioni: autodenunciarsi dinnanzi al Garante, come ha fatto l'istituto ospedaliero, e subire un'attività istruttoria che potrebbe condurre all'applicazione delle temute sanzioni, oppure far finta di nulla e continuare il trattamento.

Nonostante l'incremento delle notifiche di data breach registrato dal Garante nel 2019 rispetto all'anno precedente, recenti studi hanno anche evidenziato che, per evitare sanzioni e discredito, molte organizzazioni preferiscono non procedere alla comunicazione al Garante in caso di incidenti di sicurezza.

Probabilmente, la scelta del titolare del trattamento in questo senso dipende dal fatto che l'attività del Garante conseguente ad una notifica di un data breach viene percepita dalle organizzazioni soltanto sotto l'aspetto sanzionatorio e non come un'opportunità di revisione e miglioramento delle misure di protezione, anche sulla base dei rilievi e dei suggerimenti che l'Autorità di controllo potrebbe indicare all'esito dell'istruttoria.

In ogni caso, si tratta di violazioni sulle quali il titolare del trattamento dovrebbe quanto meno effettuare una rapida ed efficace attività di valutazione del rischio dell'incidente ed individuare le misure adeguate ad evitare future violazioni dello stesso genere.

Altro aspetto interessante della decisione in esame è che nella scelta della sanzione da applicare il Garante ha tenuto conto delle circostanze dalle quali emergeva sia l'unicità dell'episodio, sia l'accountability del titolare del trattamento, il quale immediatamente aveva provveduto ad informare l'interessato ed aveva attivato iniziative di sensibilizzazione degli autorizzati al trattamento.

Da un punto di vista meramente formale, potrebbe tutt'al più non essere condivisibile l'affermazione dell'Autorità secondo cui la notifica del data breach sarebbe stata eseguita in modo tempestivo.

L'art. 33 GDPR richiede, infatti, che la notifica della violazione dei dati personali venga effettuata senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza.

Secondo le Linee Guida del Working Party Article 29 in materia di notifica delle violazioni di dati personali (WP250) “il titolare del trattamento deve considerarsi “a conoscenza” nel momento in cui è ragionevolmente certo che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali”.

Fermo l’onere del titolare del trattamento di “prendere tutte le misure necessarie per assicurarsi di venire “a conoscenza” di eventuali violazioni in maniera tempestiva in modo da poter adottare le misure appropriate”, il Gruppo di Lavoro osserva che “il momento esatto in cui il titolare del trattamento può considerarsi “a conoscenza” di una particolare violazione dipenderà dalle circostanze della violazione. In alcuni casi sarà relativamente evidente fin dall’inizio che c’è stata una violazione, mentre in altri potrebbe occorrere del tempo per stabilire se i dati personali sono stati compromessi.”

Al riguardo, il WP29 riporta come esempio il caso di un terzo che informa il titolare del trattamento di aver ricevuto accidentalmente i dati personali di uno dei suoi clienti e fornisce la prova della divulgazione non autorizzata. Dato che al titolare del trattamento è stata presentata una prova evidente di una violazione della riservatezza, non vi è dubbio - secondo il Gruppo di Lavoro - che ne sia venuto “a conoscenza”.

Ebbene, l’esempio che precede sembra attagliarsi perfettamente al caso de quo, giacché l’istituto ospedaliero ha ricevuto una segnalazione dalla quale emergeva icto oculi la divulgazione non autorizzata dei dati clinici di un paziente che erano stati erroneamente inseriti nel fascicolo sanitario di un altro paziente.

Stante l’analogia tra l’esempio portato dal WP29 e la vicenda sottesa al provvedimento in esame, le considerazioni del Garante sul punto potrebbero essere, quindi, opinabili: l’azienda sanitaria avrebbe, infatti, potuto notificare l’incidente al Garante immediatamente dopo aver ricevuto la segnalazione, atteso che dalla stessa emergeva chiaramente il fatto che i dati sanitari di un paziente erano stati divulgati senza autorizzazione e che, ai fini della notifica al Garante, si sarebbero rivelate ininfluenti le indagini interne.

Tuttavia, è da apprezzare il fatto che il Garante abbia inteso valorizzare il comportamento proattivo tenuto dall’istituto ed abbia preferito concentrare la propria attività istruttoria su un aspetto sicuramente rilevante qual è quello della protezione dei dati sanitari, sanzionando l’Istituto per la inadeguatezza delle misure di sicurezza dalla stessa adottate. (Federprivacy)