App per diabetici: sanzionata dal Garante società statunitense

Trattati in modo illecito gli indirizzi email di circa 2000 pazienti diabetici italiani

Società statunitense usa la propria app per comunicazione illecita di dati sanitari e personali di pazienti italiani

Il Garante privacy ha sanzionato per 45.000,00 euro una società statunitense, per violazioni sui dati personali nell'utilizzo del proprio sistema di monitoraggio del glucosio e per aver comunicato illecitamente indirizzi di posta elettronica e dati sulla salute di circa 2000 pazienti diabetici italiani.

La Società ha notificato al Garante il data breach causato da un suo dipendente che, nell'ambito di una campagna informativa, ha inviato un messaggio di posta elettronica, inserendo gli indirizzi dei destinatari nel campo "cc" (carbon copy) invece che nel campo "bcc" (blind carbon copy). Ciascun destinatario ha avuto così la possibilità di visualizzare gli indirizzi email degli altri.

In base al Gdpr, ha ribadito il Garante, l'indirizzo di posta elettronica è da considerarsi un dato personale, perché riguarda una persona identificata o identificabile e va perciò trattato in modo lecito, corretto e trasparente, garantendo un'adeguata sicurezza.

Nel caso specifico, poi, considerato che la comunicazione era indirizzata a persone affette da diabete, le informazioni contenute nella email, costituivano "dati personali che possono rivelare lo stato di salute" e quindi potevano essere comunicati a terzi solo sulla base di una delega scritta dell'interessato o di un idoneo presupposto giuridico.

Nel corso dell'istruttoria l'Autorità ha rilevato ulteriori violazioni della normativa sulla protezione dei dati relative all'utilizzo del sistema di monitoraggio del glucosio. Scaricando l'apposita app, infatti, gli utenti erano chiamati ad accettare con un unico "clic" sia le condizioni contrattuali del servizio sia il contenuto dell'informativa privacy, rendendo così impossibile formulare specifici consensi per i diversi trattamenti dei dati, quale appunto quello per il trattamento dei dati sulla salute.

Violati anche i principi di correttezza e trasparenza, avendo la società fornito agli utenti un'informativa confusa e carente in molte parti essenziali. L'azienda aveva inoltre omesso di designare per iscritto il proprio rappresentante nell'Unione europea quale interlocutore per tutte le questioni privacy, come previsto dal Regolamento.

Nel valutare la sanzione da applicare alla società, il Garante ha tenuto conto della mancanza di intenzionalità nell'invio dell'email e del comportamento collaborativo della compagnia. In ottemperanza alle prescrizioni del Garante, l'Azienda dovrà conformare i trattamenti di dati personali alla normativa vigente e rielaborare l'informativa sulla privacy in una forma concisa, trasparente e comprensibile, comunicando le iniziative intraprese in tal senso.

Fonte: Garante Privacy