

Qualche informazione sulle sanzioni GDPR in altri paesi

Alberghi, banche e società finanziarie, compagnie aeree e società di taxi; ma anche sanità ed enti pubblici nel mirino dei garanti della privacy europei. E in giro per il Vecchio continente stanno fioccando sanzioni per violazioni degli adempimenti imposti dal Regolamento Ue sulla protezione dei dati (2016/679), tra cui spiccano quelli sulla sicurezza dei sistemi informativi. Un regolamento che è direttamente applicabile anche in Italia e che è ormai entrato a regime dal 25 maggio 2018. Ma vediamo quello che sta capitando negli stati dell'Unione.



GRAN BRETAGNA - Notificata a un gruppo alberghiero l'avviso di procedimento finalizzato all'applicazione di una sanzione di oltre 99 milioni di sterline a seguito di un attacco informatico. La stessa società ha notificato al garante inglese (Ico) la violazione della sicurezza risalente al novembre 2018, che ha messo a rischio 339 milioni di informazioni, di cui circa 30 milioni relative a persone residenti in Europa. Probabilmente il fatto risale al 2014 ed è stato ereditato da una precedente catena acquisita nel corso di un'operazione societaria. Secondo il garante inglese la società non ha fatto le opportune verifiche e non ha messo in sicurezza i sistemi. Il procedimento è ancora in fase di istruttoria e l'Ico non ha assunto la decisione finale. Un altro episodio ha coinvolto una compagnia aerea. Qui si tratta di importi più bassi in relazione al minor numero di persone potenzialmente coinvolte (circa mezzo milione) e ha riguardato sempre un data breach iniziato probabilmente a giugno 2018. Al centro dei controlli la scarsa sicurezza a riguardo di accessi a internet, pagamenti online, dettagli delle prenotazioni aeree e dati identificativi dei passeggeri. Anche qui il procedimento è in corso.

BELGIO - Il garante della privacy belga ha ammonito il servizio sanitario pubblico per non avere risposto alla richiesta di accesso di un cittadino. Quest'ultimo ha chiesto di avere copia dei propri dati personali in relazione a una procedura di nomina quale componente di una commissione medica locale. Nel silenzio dell'ente sanitario, il garante belga ha adottato la misura correttiva. Il garante belga ha, poi, applicato una sanzione di 2 mila euro per violazione del trattamento di dati nell'ambito di campagna elettorale. Un amministratore locale ha utilizzato, per fini di propaganda, dati ottenuti durante l'esercizio del mandato.

Secondo il garante belga un conto è la corrispondenza istituzionale, un altro è utilizzare la e-mail ricevuta per inviare con il comando «rispondi» messaggi di propaganda elettorale.

LITUANIA - Il garante lituano ha ingiunto il pagamento di 61 mila euro a una banca per un data breach. In questo caso i dettagli della movimentazione della clientela sono stati disponibili in chiaro per più di due giorni tramite internet. Durante le indagini è emerso anche che la banca raccoglie più dati di quelli necessari per i servizi forniti.

FINLANDIA - Due casi hanno coinvolto banche e società finanziarie. Entrambe hanno riguardato una non corretta profilazione della clientela in relazione al giudizio di meritevolezza del credito. In contestazione il dato sull'età del richiedente il prestito. Secondo il garante finlandese il mero dato dell'età non è idoneo a descrivere la solvibilità e ha ordinato alla banca di cambiare il sistema automatizzato di istruttoria delle richieste di credito.

POLONIA - Il garante polacco ha comminato 220 mila euro di sanzione a una società che non aveva dato l'informativa privacy agli interessati: oltre 6 milioni gli interessati. I dati erano stati raccolti da fonti disponibili al pubblico e trattati per scopi commerciali. L'informativa è stata inviata solo ai soggetti di cui la società aveva l'indirizzo di posta elettronica (un'esigua minoranza). E questo non è bastato ad evitare sanzioni.

ROMANIA - In tre casi il garante rumeno ha applicato sanzioni pecuniarie. Nel primo episodio la violazione da parte di una società privata ha riguardato le norme sulla sicurezza dei trattamenti. L'importo della sanzione è stato modesto (3 mila euro). Il garante rumeno ha accertato che il deficit di sicurezza la diffusione su internet di dati personali nei mesi di dicembre 2018 e gennaio 2019. Nel secondo caso la violazione è stata la stessa, ma la sanzione è stata più alta (15 mila euro). Qui si è trattato di una lista stampata su carta, usata per controllare clienti di un hotel al momento dell'ingresso alla sala ristorante per la colazione (in totale 46 persone). La lista è stata fotografata e diffusa. Il terzo episodio ha coinvolto una banca e si è trattato della violazione dell'articolo 25 Gdpr (privacy by design e by default). La sanzione è stata di circa 130 mila euro. La mancata conformità ai principi di sicurezza e minimizzazione del trattamento dei dati ha esposto i clienti alla acquisizione indebita dei dati identificativi personali e della movimentazione. Interessati dalla vicenda sono state oltre 337 mila persone.

DANIMARCA - Il garante danese ha aperto una procedura contro un'azienda di arredi per non avere cancellato i dati di 385 mila clienti, conservati in un vecchio sistema informativo, non più in uso, perché sostituito da altro aggiornato. Il garante danese ha anche aperto un procedimento per l'applicazione di una sanzione di 160 mila euro alla compagnia di taxi, per mancata cancellazione dei dati della prenotazione delle corse. La società aveva la regola interna di distruzione dei dati dopo due anni. Ma questo non è avvenuto, in quanto la società cancellava solo i nomi, ma non i numeri di telefono dei clienti.

NORVEGIA - Il garante norvegese ha comminato una sanzione di 170 mila euro a un comune, reo di non avere protetto 35 mila credenziali di accesso al sistema informativo municipale, in particolare relativi a studenti e dipendenti delle scuole primarie.

AUSTRIA - Nel mirino del garante austriaco la società del servizio postale per plurime violazioni: raccolta di dati sulle convinzioni politiche, lacune nella redazione della valutazione di impatto privacy (Dpia).