CONSULENTI DI DIREZIONE ASSOCIATI

GDPR, prime sanzioni in Europa: quale lezione trarre per le aziende

In attesa di conoscere quale sarà la sanzione che il Garante europeo comminerà alla catena alberghiera Marriot per il recentissimo caso di data breach che riguarda i dati personali di ben 327 milioni di persone, sono arrivate inesorabili le prime sanzioni in Europa ad alcune aziende, private e pubbliche, che non hanno ottemperato alle disposizioni del GDPR, entrato in vigore ormai da sei mesi.

Ecco quale lezione possiamo trarne…e ne dovrebbero trarre le aziende.

Le prime multe per violazione del GDPR

Partendo dalla "meno costosa", nel mese di ottobre il Garante austriaco Datenschutzbehörden, ha erogato, a seguito di una ispezione, una sanzione di 4 mila euro ad una azienda che utilizzava il sistema di video sorveglianza in malo modo, puntandolo in parte sul marciapiede esterno al perimetro aziendale riprendendo in modo eccessivo, senza alcuna giustificata motivazione e senza informare con apposita cartellonistica i passanti.

Anche la prima sanzione ad oggetto data breach è stata erogata a novembre dal Garante tedesco Der Landesbeauftragte für Datenschutz und Informationsfreiheit ad una azienda tedesca che, dopo aver dichiarato l'avvenuto data breach riguardante ben 330 mila credenziali di caselle di posta elettronica di cittadini tedeschi, è stata multata con una sanzione di 20 mila euro. In questo caso l'attaccante, oltre ad aver sottratto le credenziali utente comprensive di password, le ha anche divulgate in chiaro sulla rete Internet mettendole a disposizione di chiunque; proprio per questo motivo l'autorità tedesca ha sanzionato l'azienda non tanto per l'avvenuta violazione dei sistemi informatici, ma per il fatto che le password delle caselle di posta elettronica venivano salvate in chiaro all'interno della base dati senza l'utilizzo di opportuni sistemi di cifratura.

In Portogallo la comissão nacional de proteccao de dados ha erogato a una struttura ospedaliera nazionale la sanzione più alta di cui ad oggi abbiamo notizia, ben 400 mila euro. La multa è stata data a seguito di un controllo ispettivo che ha permesso di accertare che sui sistemi informativi della struttura ospedaliera vi erano seri problemi di politiche di accesso al dato, evidenziato come, psicologi, infermieri e medici di qualsiasi reparto potevano, non soltanto accedere, ma anche modificare con estrema facilità (e in totale assenza del principio di necessità) i dati personali e sanitari contenuti nelle cartelle cliniche di tutti i pazienti che sono stati ospiti del complesso ospedaliero; sempre durante l'ispezione gli auditor hanno evidenziato una inadeguata politica di accesso al dato, evidenziando come il problema non è tanto sulla configurazione del sistema informativo ma soprattutto sulla inadeguatezza della policy di accesso al dato scelta e divulgata a tutti gli operatori della struttura ospedaliera.

Le lezioni che le aziende italiane possono trarre

Quali sono gli spunti di riflessione che le aziende italiane devono trarre da questi episodi? Sicuramente che le tante attese sanzioni sono arrivate e che per adesso sono state inesorabili; basti pensare all'episodio austriaco, una problematica quella della cartellonistica informativa inerente alla video sorveglianza spesso sottovalutata dalle pmi e micro imprese italiane che, probabilmente per mancanza di tempo o per la poca attenzione alla tematica della privacy, non hanno mai adeguato le informative riguardanti le aree sottoposte a video sorveglianza, in alcuni casi omettendo (tutt'oggi) l'esposizione dei cartelli informativi nei luoghi dove vi è un sistema di video sorveglianza in funzione. La sanzione data all'azienda tedesca ci fa capire come le autorità garanti per la protezione dei dati non erogheranno sanzioni per la sola avvenuta violazione ai sistemi che custodiscono e trattano dati personali, se non nel momento in cui, a fronte di un accertamento, si evidenziassero gravi problematiche di cyber security, come per l'appunto, il madornale errore di conservale la password di un account in chiaro all'interno delle memorie informatiche aziendali, senza alcun ausilio di ormai consolidati sistemi di cifratura. Una riflessione in più va fatta in considerazione

alla cattiva abitudine delle aziende italiane che adottano una politica per la gestione del data breach (o dell'incidente informatico) troppo generalista che non tiene in considerazione il fatto che nella maggior parte dei casi l'azienda ha una politica per la gestione dell'incidente informatico ma non ha un sistema per identificare gli attacchi informatici e per capire che sta avvenendo un attacco informatico che potrebbe a sua volta scaturire un data breach. Non per ultimo il caso portoghese ci deve far riflettere su quale possa essere l'attuale stato dei sistemi informativi delle aziende sanitarie, private e pubbliche, del nostro territorio. Nel nostro territorio esistono regioni e strutture virtuose che sono al passo con i tempi e con le norme, ma per esperienza personale dello scrivente, la situazione in molti altri casi è la medesima dell'azienda ospedaliera portoghese, con addirittura alcune realtà che tutt'oggi, da nord a sud, sperano di non ricevere mai alcuna ispezione del Garante nemmeno nel2019, perché lo stato dell'arte della revisione delle politiche di accesso al dato e dell'attuazione di queste politiche all'interno del sistema informativo aziendale è ancora in una fase embrionale, tra sistemi e software obsoleti non aggiornabili, personalizzazioni di software necessarie per l'interoperabilità del dato che generano modalità lasche di accesso al dato stesso, e chi più ne ha più ne metta. Non ci sono più scuse, e i fatti appena accaduti testimoniano un impegno dei Garanti degli Stati membri nel mantenere la guardia sempre alta, a tutela dei dati dei cittadini. Le aziende italiane sono avvisate, ancora una volta, grazie alle disavventure di altri. Colgano tutti l'occasione per imparare dagli errori e impegnarsi nell'ottemperanza della norma, sia dal punto di vista delle politiche e dei regolamenti aziendali, sia dal punto di vista implementativo e tecnologico.