PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 18 - numero 3787 di martedì 24 maggio 2016

Chi ha bisogno di un responsabile della protezione dei dati?

Il 24 maggio 2016 entra in vigore il nuovo regolamento generale europeo sulla protezione dei dati 679/2016. Le nuove regole si applicano ai nuovi trattamenti, mentre per i trattamenti già in corso vi è tempo fino al 24 maggio 2018. Di Adalberto Biasiotti.

Durante un recente webinar sono state molte le domande che mi sono state poste, afferenti a tempi e modi di entrata in vigore delle nuove ed avanzate disposizioni del regolamento europeo 679/2016. Un aspetto che merita particolare attenzione è legato alla designazione del responsabile della protezione dei dati, soggetto del tutto sconosciuto in Italia ma già noto in altri paesi.

Pubblicità
<#? QUI-PUBBLICITA-MIM-[CODE] ?#>

Trascrivo letteralmente l'articolo specifico del regolamento:

Articolo 37 Designazione del responsabile della protezione dei dati
1. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:
a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure
c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10. omissis

Sulla base del principio che questo obbligo di designazione non si applica a trattamenti già in essere, in quanto vi è un periodo di grazia che si estende fino a 24 maggio 2018, appare evidente che ogni nuovo trattamento che viene svolto dai titolari sopra elencati, o che ha per oggetto le attività sopra elencate, deve necessariamente essere sottoposto al vaglio di un responsabile della protezione dei dati.
Un altro articolo illustra in dettaglio le competenze, le responsabilità ed i compiti di questo nuovo soggetto, che dà indubbiamente un grande contributo al miglioramento delle modalità di trattamento di dati personali.
Si faccia attenzione alla differenza significativa che esiste nelle tre lettere del comma uno.
Mentre la lettera a) impone l'obbligo di designazione ad un qualsivoglia titolare, quale che siano i trattamenti che egli svolge, se è un'autorità o un organismo pubblico (ad eccezione ad esempio delle procure della Repubblica), le lettere b) C) non fanno riferimento ad una specifica categoria di titolari, ma fanno riferimento al tipo di trattamento che il titolare svolge.

Mi sembra del tutto legittimo ritenere che una grande catena di supermercati, che emette tessere di fedeltà con attribuzione di punteggi, analisi di acquisti a premio e altre attività similari, applicabili a decine di migliaia di clienti, debba necessariamente designare un responsabile della protezione dei dati personali.

Parimenti, una grande catena di istituzioni sanitarie private, che gestisce dozzina di cliniche ed ambulatori in varie parti d'Italia, indubbiamente tratta su larga scala dati personali particolari (*art. 9 - dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*) dovrà necessariamente designare un responsabile della protezione dei dati. Stesso ragionamento si applica certamente i sindacati.

Se il trattamento è già in corso, si potrà aspettare fino alla data ultima di entrata in vigore, ma credo proprio che potrebbe essere un'idea non particolarmente brillante.

Chiudo infine questo intervento segnalando che non bisogna soltanto esaminare i casi in cui la designazione di questo responsabile è obbligatoria, ma bisogna utilizzare lungimiranza e buon senso, uniti alla diligenza del buon padre di famiglia, valutando attentamente l'opportunità di designare un responsabile della protezione dati personali anche dove tale designazione non è obbligatoria per legge, ma è certamente opportuna!

24 maggio 2018: data fatidica

Sarà quindi il 24 maggio 2018 la data ultima entro la quale dovranno essere adottate tutte le indicazioni del nuovo regolamento europeo sulla protezione dei dati personali, che sono decisamente più impegnative e vincolanti, rispetto a quelle dell'attuale decreto legislativo 196/2003.
Il regolamento introduce nuove responsabilità, rafforza i diritti degli interessati e pone dei limiti al movimento internazionale dei dati.
Come abbiamo già accennato, sono più di 28.000 i responsabili della protezione dei dati personali, di cui le aziende avranno bisogno, in tutta Europa. Ricordiamo anche che la stima è alquanto prudenziale.
Vi sono alcuni passi che le aziende possono già cominciare a prendere, per avviare il processo di rispetto delle nuove indicazioni del regolamento.
Il primo passo è evidentemente quello di fare una completa rassegna di tutti i dati personali che vengono trattati, le modalità di trattamento, le modalità di archiviazione e ,fattore di cui poco sino ad oggi i titolari si sono preoccupati, indicare un termine entro il quale i dati dovranno essere cancellati.
Occorre cominciare ad individuare un responsabile per la protezione dei dati personali, a fronte di un'offerta che per ora è decisamente insufficiente, rispetto alla domanda.
Occorre attivare al più presto un piano per fronteggiare possibili violazioni dei dati, che in precedenza doveva essere attivato solo per gli operatori delle telecomunicazioni, mentre oggi invece il piano deve essere chiamato in causa a fronte di qualsiasi violazione. Se la violazione ha caratteristiche di particolare gravità ed impatto sugli interessati, occorre anche avviare fin da adesso un piano per informare gli incaricati del fatto che i loro dati sono stati violati.

Non mancherò di tenere aggiornati i lettori sulla graduale applicazione dei dettati del regolamento, che dovrà essere integrato da disposizioni nazionali, assunte dalle autorità Garanti, ma inquadrate in un processo di coerenza, che obbliga le stesse autorità a confrontarsi con le altre autorità europee e, soprattutto, con il neocostituito comitato europeo per la protezione dei dati.

Adalberto Biasiotti

Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

Direttiva (Ue) 2016/680 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio

Questo articolo è pubblicato sotto una Licenza Creative Commons.

www.puntosicuro.it