PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 19 - numero 4133 di Giovedì 30 novembre 2017

Il punto sulla normativa in materia di protezione dei dati personali

Un elenco delle normative oggi disponibili in materia di protezione di dati personali: un punto aggiornato ed accurato sulla situazione.

Pubblicità
<#? QUI-PUBBLICITA-MIM-[BIA0001] ?#>

È appena il caso di ricordare a tutti i lettori che il 25 maggio 2018 entrerà pienamente in vigore il regolamento generale europeo in materia di protezione dei dati personali, abolendo di fatto ogni precedente pronunciamento, che possa anche potenzialmente essere in contrasto con le disposizioni del regolamento, valide ed uguali in tutti i paesi europei.

Per facilitare la applicazione del regolamento, numerosi comitati normativi si sono attivati, soprattutto a livello europeo, per mettere a disposizione dei titolari, dei responsabili del trattamento e dei responsabili della protezione dei dati un coacervo normativo, che possa costituire il cosiddetto "stato dell'arte".

L'autorità garante nazionale si è pure attivata, non solo dando indicazioni alle pubbliche amministrazioni sulle misure che fin da adesso esse possono attuare, per cominciare a rispettare il nuovo regolamento, ma anche per mettere a punto le procedure che permetteranno di accreditare gli organismi di certificazione, che potranno rilasciare certificati di conformità a norme italiane europee.

La situazione non è molto diversa da quella che abbiamo già vissuto, quando il ministero dell'interno ha deciso di imporre agli istituti di vigilanza di essere certificati secondo norme, di valenza italiana o oppure europea, affidando l'incarico di certificazione a istituti debitamente selezionati e qualificati.

Il problema quindi non riguarda tanto la stesura della norma, che viene effettuata solo dai comitati europei, ma la messa a punto di procedure di certificazione e di riconoscimento di organismi accreditati.

In allegato a questo documento metto a disposizione di tutti i lettori un elenco delle normative oggi disponibili, a livello mondiale, vale a dire normative emesse dalla International standard organization, oppure a livello europeo, vale a dire normative emesse dal comitato europeo di normazione.

Come di consueto, come ben sa chiunque deve mettere a punto un piano di protezione di un bene, sia di tipo materiale, sia di tipo immateriale, il primo passo da attuare è quello di effettuare una valutazione di rischio, determinando il livello di rischio esistente, in funzione del prodotto della frequenza prevista del verificarsi del rischio, moltiplicato per il danno che il verificarsi del rischio potrebbe creare.

Bene tre norme sono dedicate a questo aspetto, che rappresenta un passo fondamentale, senza il quale tutte le norme successive, che indicano rimedi, non saprebbero a che rischio applicarsi.

Successivamente vengono messe a disposizione delle norme, alcune solo a livello di bozza, in attesa dell'approvazione ufficiale, che sono perlopiù indirizzate alla tecnologia dell'informazione.

Oggi sappiamo tutti che la grande maggioranza dei dati personali viene trattata con sistemi informatici e quindi non deve stupire alcuno il fatto che la protezione dei dati, su supporto informatico, richieda un'attenzione tutta particolare.

Altre norme invece sono dedicate a garantire un soddisfacente livello di sicurezza, sempre perlopiù informatica, in settori specializzati, come ad esempio il settore sanitario e il settore dei sistemi intelligenti di trasporto.

Le statistiche disponibili a livello mondiale hanno già messo in evidenza come il settore della sanità rappresenti una delle aree più deboli esistenti, in materia di protezione dei dati personali.

Questa è la ragione per la quale molti comitati tecnici si sono concentrati nella messa a disposizione di procedure efficienti ed efficaci.

D'altro canto, finché un primario afferma che a lui interessa di più la salute di un paziente, piuttosto che la protezione dei dati personali, non ci si può stupire se il settore sanitario presenti questi gravi problemi.

Parimenti importante è il settore dei servizi finanziari, per la ovvia necessità di proteggere i preziosi dati dei clienti. Anche in questo caso, sono già disponibili delle normative di grande efficacia.

Infine, appare evidente che oggi i dati personali, su supporto informatico, non si trovano solo custoditi all'interno dei server del titolare del trattamento, ma vengono spesso custoditi nel cloud, per una serie di ragioni che non è il caso di approfondire.

A questo punto, sembra del tutto legittimo che il titolare del trattamento, il responsabile del trattamento e il responsabile della protezione dei dati individuino dei parametri che permettano di valutare quale sia la competenza e l'affidabilità di un gestore di un servizio nel cloud.

Questo elenco è completato dalle linee guida per i fabbricanti di dispositivi, dotati di connessione Internet, i famosi apparati IoT, nonché un interessantissimo documento, che risale a gennaio 2015, che mette in evidenza come gli organi sportivi, che devono

prelevare e tenere sotto controllo campioni organici di atleti, sospetti di doping, debbano proteggere questi dati oltremodo critici.

Una perdita o un'alterazione di questi dati potrebbero portare al ritiro di una medaglia olimpica e si può ben capire come questi dati meritino la massima protezione possibile.

A tutti i lettori, buon lavoro e rapida applicazione di queste preziose norme.

Vedi allegato (pdf, 34 kB)

Adalberto Biasiotti

 Questo articolo è pubblicato sotto una Licenza Creative Commons.

---

www.puntosicuro.it