PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 20 - numero 4352 di Venerdì 16 novembre 2018

Le certificazioni in tema di protezione dei dati: alcuni dubbi

Facciamo il punto sulla situazione dei nuovi strumenti di sicurezza introdotti dal regolamento generale sulla protezione dei dati, come i processi di certificazione.

Il regolamento generale sulla protezione dei dati ha introdotto il concetto di certificazione, vale a dire la possibilità di validare la correttezza delle modalità di trattamento dei dati personali, da parte dei titolari.

Il titolare può utilizzare un codice di condotta, debitamente certificato, oppure altri strumenti di sicurezza, anch'essi certificati, dall'autorità Garante nazionale oppure da un ente terzo approvato dalla stessa autorità Garante.

Il nostro Garante si è attivato e nel decreto legislativo 101/2018 è stato riconosciuto, come organo nazionale di accreditamento, Accredia. Quest'organo nazionale potrà a sua volta delegare ad istituti di certificazione lo svolgimento di attività di controllo circa il puntuale rispetto di codici di condotta o altri strumenti di sicurezza, come ad esempio la serie normativa ISO 27000, da parte dei titolari.

Nel tentativo di armonizzare le varie iniziative, che potrebbero essere attivate dai Garanti nazionali in ogni paese europeo, la agenzia europea per la sicurezza di sistemi informativi ? ENISA - ha pubblicato delle linee guida, che danno indicazioni sulle modalità con cui è possibile individuare e validare i processi di certificazione.

Come i lettori già sanno, il regolamento generale è uno strumento di armonizzazione del regime di trattamento dei dati nell'intera Europa e mette a disposizione strumenti, anch'essi validi nell'intera Europa, per aiutare i titolari nel rispetto delle disposizioni del regolamento. La possibilità di certificare tecniche di protezione dei dati, l'utilizzo di sigilli e marchi rappresentano strumenti garantistici, a disposizione dei titolari. È evidente che questi strumenti possono offrire un aiuto non indifferente ai titolari, nel raggiungere e dimostrare piena conformità con le indicazioni del regolamento generale.

Un vantaggio addizionale di questi schemi di certificazione è quello di migliorare il livello di trasparenza nei confronti degli interessati, che potranno così rapidamente verificare il livello di protezione dei dati, offerto da uno specifico titolare.

Per questa ragione ENISA ha pubblicato un rapporto, che permette di identificare ed analizzare le sfide che devono essere superate dai meccanismi di certificazione della protezione dei dati, analizzando anche schemi già esistenti.

Ricordo ai lettori che la certificazione, come attività di valutazione di conformità allo schema, viene svolta necessariamente da un soggetto terzo, vale a dire un istituto di certificazione.

Le competenze dell'istituto di certificazione vengono convalidati dall'autorità Garante nazionale o da un ente nazionale di accreditamento.

Al termine di un processo di certificazione, con esito positivo, viene emesso un certificato, od un sigillo, che conferma che il titolare coinvolto soddisfa i requisiti richiesti dello schema di certificazione. Nulla impedisce che in futuro questi schemi possano essere recepiti in normative europee.

La certificazione può essere obbligatoria, se è indicata dalla legge, oppure inserita in un capitolato di appalto, o volontaria in altri casi.

È evidente che il processo di certificazione si inserisce positivamente nel principio di responsabilizzazione del titolare e del responsabile ed ecco la ragione per la quale è possibile che siano sempre più numerosi i titolari, che faranno ricorso a questo strumento, che dimostra la loro diligenza nell'attuare i principi di protezione dei dati personali, affidati dagli interessati.

Al momento, esistono già in Europa numerosi schemi di certificazione, ma non in Italia.

O almeno, questi schemi di certificazione sono esistenti anche in Italia, con specifico riferimento alla serie normativa ISO 27000.

In altri paesi, esistono sigilli, come ad esempio Europrise, oppure sigilli offerti dalle autorità nazionali Garanti, come ad esempio il CNIL in Francia e l'ICO nel Regno Unito.

È bene prestare attenzione al fatto che le certificazioni che fanno riferimento agli aspetti gestionali possono essere diverse dalla certificazione, che riguardano il trattamento vero e proprio.

Il meccanismo di protezione dei dati del regolamento europeo, illustrato negli articoli 42 e 43, può essere considerato come un processo di certificazione con precisi obiettivi. L'obiettivo non è solo quello di verificare se particolari misure sono attuate, ma anche di verificare se queste misure sono sufficienti per garantire un adeguato livello di protezione dei dati, definito dopo aver condotto un'analisi di rischio.

L'analisi condotta da ENISA ha messo in evidenza come vi siano ancora differenze significative tra i vari paesi ed ecco perché il documento si chiude con alcune raccomandazioni significative, appresso elencate.

- Le autorità di certificazione nazionali e le autorità Garanti nazionali, con il supporto della commissione europea e del comitato europeo per la protezione dei dati, devono individuare un approccio comune allo sviluppo di meccanismi di certificazione della protezione dei dati.

- Il comitato europeo per la protezione dei dati, operando in stretto collegamento con le autorità nazionali, deve promuovere uno schema generale europeo di certificazione, conforme a criteri largamente condivisi.

- Le autorità Garanti nazionali e gli enti di certificazione, con il supporto del comitato europeo per la protezione dei dati e della Commissione europea, devono offrire linee guida in grado di garantire la coerenza e l'armonizzazione di questi meccanismi di certificazione, in varie parti dell'Europa.

- I processi di certificazione devono essere affidabili e trasparenti, sotto il controllo della Commissione europea e del comitato europeo per la protezione dei dati.

- Occorre stimolare in ogni modo lo scambio di informazioni ed esperienze maturate, in fase di applicazione degli schemi di certificazione nei vari paesi, per migliorare il livello qualitativo generale di questi processi di certificazione europei.

Allegato doc Enisa (pdf)

Adalberto Biasiotti
