PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 18 - numero 3851 di martedì 13 settembre 2016

Privacy: dal Regolamento alle Linee Guida comportamentali

Come intraprendere il percorso di conformità al nuovo Regolamento Europeo di Protezione dei Dati Personali? I cambiamenti necessari entro il 25 maggio 2018. Di Paola Limatola e Sebastiano Plutino.

Il 25 maggio 2016 è entrato in vigore il nuovo Regolamento EU 679/2016 "Protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati" che abroga la direttiva 95/46/CE ("Regolamento generale sulla protezione dei dati") sulla protezione dati personali.

Il Regolamento diventerà obbligatorio dal 25 maggio 2018 ma, nel frattempo, può essere adottato e può essere utilizzato in parallelo all'attuale Codice Protezione Dati Personali (Dlgs 196/2003).

Le imprese avranno quindi due anni di tempo per intraprendere il percorso di miglioramento e adottare i cambiamenti necessari al fine di adeguare il loro sistema di gestione dei dati personali dotandosi di strumenti attuativi ed operativi per raggiungere l'obiettivo di ridurre l'eventuale impatto delle sanzioni applicabili dall'Autorità.

Rispetto al Codice (Dlgs 196/2003), il Regolamento obbliga ad una maggiore attenzione e ad una maggiore trasparenza verso gli interessati; questo implica che ciascuna organizzazione deve avviare le necessarie modifiche ai processi e ai sistemi interni, analizzando attentamente lo stato attuale, gestendo le modifiche da apportare - con la dovuta attenzione ai costi interni - e dosando quindi opportunamente e correttamente gli sforzi.

All'articolo 40 il Regolamento permette, anzi raccomanda, l'elaborazione e l'adozione di Codici di Condotta, definendoli strumenti "destinati a contribuire alla corretta applicazione" della nuova normativa; i Codici di Condotta vanno sottoposti all'Autorità (Autorità Garante Protezione Dati Personali per l'Italia) responsabile di emettere un parere di conformità, e la loro osservanza può essere monitorata da un organismo in possesso del livello adeguato di competenza (art. 41).

I Codici di Condotta hanno caratteristiche simili a quelle dei Codici Deontologici, che oggi fanno parte del Dlgs 196/2003: analogamente a quanto accaduto per i suddetti Codici Deontologici, annessi alla normativa vigente, è probabile che l'Autorità Garante faccia propri i Codici di Condotta conformi e li renda disponibili ("registra e pubblica" sostiene il punto 6 dell'art. 40) favorendo i processi di monitoraggio e certificazione.

Sempre il Regolamento, all'art. 42, incoraggia l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dati, allo scopo di dimostrare la conformità al Regolamento dei trattamenti effettuati; la certificazione deve essere rilasciata da organismi accreditati e in possesso di un adeguato livello di competenze (art. 43) sulla base di un meccanismo di certificazione approvato.

Di fatto il Codice di Condotta, partendo dal Regolamento, traccia la strada per la definizione di un Sistema di Gestione della Protezione dei Dati Personali: l'adozione di un Sistema di Gestione, come accaduto in altri ambiti (Qualità, Ambiente, Salute e Sicurezza sul Lavoro, Sicurezza delle Informazioni) innesca un processo di miglioramento virtuoso da cui ogni impresa può trarre beneficio.

Codici di Condotta e certificazioni sono quindi uno strumento a disposizione di tutte le organizzazioni - grandi, medie e piccole ? che effettuano trattamento di dati personali in ogni settore di mercato per attestare, in modo indipendente, il corretto comportamento verso gli interessati e verso l'Autorità.

Ciascuna organizzazione in possesso delle caratteristiche previste all'art. 40 può sviluppare un Codice di Condotta e presentarlo all'Autorità Garante per la Protezione Dati Personali per chiedere un parere di conformità.

In alternativa, l'organizzazione ha l'opportunità di adottare un Codice di Condotta già esistente e ritenuto conforme dall'Autorità Garante, integrandolo con proprie Linee Guida Operative che hanno lo scopo di calare il Codice di Condotta nella specifica realtà dell'organizzazione. Le Linee Guida operative devono, quindi, illustrare in dettaglio le attività dell'organizzazione atte a favorire la gestione del trattamento dei dati personali in modo standardizzato e attraverso indicazioni puntuali.

L'efficace adozione di questo strumento (il Codice di Condotta appunto) può essere monitorata e/o certificata da appositi organismi, in linea con quanto detto in riferimento agli articoli 41 e 42 del Regolamento.

Tale monitoraggio e, meglio ancora, la certificazione, può permettere all'organizzazione di dotarsi di un "bollino/marchio" di certificazione riconosciuto che consente alla stessa di ridurre l'impatto di possibili sanzioni (ai sensi dell'art. 83 comma 2j) a seguito di verifica (similarmente a quanto avviene alle organizzazioni regolarmente certificate OHSAS 18001).

In linea con quanto previsto dal Regolamento, sono stati recentemente sottoposti all'attenzione dell'Autorità Garante due importanti strumenti fra loro connessi: il Codice di Condotta DPMS 44001:2016® e il Meccanismo di Certificazione DPMC 44002:2016® sui quali si è in attesa dell'emissione del parere da parte della all'Autorità Garante.

E' tuttavia importante sottolineare che, nonostante la data del 25 maggio 2018 sembri ancora lontana, è importante e utile per le organizzazioni intraprendere il percorso di conformità al nuovo Regolamento Europeo.

Le attività che la singola impresa dovrà svolgere per l'adeguamento legislativo dipenderanno da molti fattori: saranno legate, ad esempio, alla specificità del settore in cui opera l'organizzazione, alla tipologia di clientela servita, alla tipologia dei dati trattati, alle modalità di trattamento, alla obbligatorietà di dotarsi della professionalità di un Data Protection Officer (DPO=Responsabile della Protezione Dati Personali) nei casi previsti dal Regolamento.

Non esistono ricette facili o risposte buone per ogni occasione: il lavoro da fare dovrà essere valutato caso per caso e potrà anche, in alcuni casi, tradursi in un impegno significativo di tempo e risorse per l'organizzazione.

L'adozione di un Codice di Condotta e l'eventuale predisposizione di apposite Linee Guida Operative sono l'opportunità per una valutazione ragionata - approccio al rischio come definito dai nuovi sistemi di gestione - del cammino da percorrere in vista del 25 maggio 2018 e l'occasione per una attenta pianificazione dei cambiamenti e delle migliorie da apportare al proprio sistema di gestione del trattamento dei dati personali.

L'organizzazione che volesse intraprendere questo percorso fornirebbe un messaggio di trasparenza e di impegno nei confronti della propria clientela e dei propri stakeholders (in senso più ampio) e potrebbe ricavarne un vantaggio competitivo in un mercato che è sempre più internazionalizzato.

Paola Limatola

Sebastiano Plutino

---

www.puntosicuro.it