ISO/IEC 27701, la norma internazionale per certificare la protezione dei dati personali

Author : Fabio Guasconi

Date : 12 Settembre 2019

Durante il mese di agosto 2019 ha finalmente visto la luce una **norma molto attesa**, i cui lavori erano iniziati già nel lontano 2016 e che, dopo diversi cambi di titolo e anche di numerazione, è infine risultata essere la:

"*ISO/IEC 27701 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*".

La forte attesa per questa norma è motivata da più elementi, il primo dei quali è l'argomento, che la colloca in un segmento di mercato in forte evoluzione quale quello delle certificazioni secondo l'art.42 del Regolamento UE 679/2016 per la protezione dei dati personali (d'ora innanzi GDPR). Il secondo motivo è il comitato che l'ha pubblicata, ISO/IEC JTC 1 SC 27 (WG 5), recentemente rinominato "*Information Security, Cybersecurity and Privacy Protection*". Questo comitato, essendo lo stesso che ha creato e manutiene la ISO/IEC 27001, la ISO/IEC 15408 e 200 altre norme tecniche massimamente rilevanti in questo ambito a livello internazionale dal lontano 1989, è certamente una delle fonti autorevoli più importanti al mondo e lo stesso fatto che abbia deciso di intraprendere dei lavori in questo senso la dice lunga sulla loro prevista strategicità.

La nuova ISO/IEC 27701, fino a pochi giorni prima della pubblicazione identificata con il numero 27552 e poi passata a un numero da "*testa di serie*" per i sistemi di gestione, è impostata secondo quanto prescritto dalla ISO/IEC 27009 come una **norma "*sector specific*"** che va quindi a contestualizzare le prescrizioni generali della ISO/IEC 27001 nell'ambito specifico della protezione dei dati personali, aggiungendovi sia dei requisiti sia delle linee guida.

Questo approccio da una parte rende più facile l'adozione della ISO/IEC 27701 laddove già esista un sistema di gestione per la sicurezza delle informazioni conforme alla ISO/IEC 27001 mentre, dall'altro, richiede lo sforzo di implementare *ex novo* tale sistema qualora non sia già esistente, cosa che tipicamente comporta **costi e tempi non trascurabili.**

Il testo della ISO/IEC 27701, tolti i primi capitoli introduttivi, è articolato in quattro capitoli principali (5, 6, 7, 8), rispettivamente relativi a:

- requisiti specifici per il sistema di gestione per la protezione dei dati personali collegati alla ISO/IEC 27001;
- linee guida per il sistema di gestione per la protezione dei dati personali collegate alla ISO/IEC 27002;
- linee guida aggiuntive alla ISO/IEC 27002 per i titolari;
- linee guida aggiuntive alla ISO/IEC 27002 per i responsabili.

In sostanza la norma **aggiunge una serie di requisiti** alla ISO/IEC 27001 nel capitolo 5 per estendere il sistema di gestione dalla sola sicurezza delle informazioni a tutto l'ambito della protezione dei dati personali, richiedendo ad esempio di considerare esplicitamente i trattamenti ed i ruoli in essi legalmente coperti dall'organizzazione e di valutarne i rischi non solo relativamente a disponibilità, integrità e riservatezza delle informazioni ma anche al rispetto dei diritti e delle libertà degli interessati. Questa sezione è l'unica che specifica requisiti: quindi l'unica da rispettare in ogni caso per poter dichiarare la conformità alla ISO/IEC 27701.

Nel capitolo 6 sono invece riportate, per ogni controllo della ISO/IEC 27002, delle linee guida aggiuntive per l'attuazione del controllo stesso inerenti alla protezione dei dati personali. Per il controllo 5.1.1 relativo alle politiche per la sicurezza delle informazioni, ad esempio, viene suggerito di inserire, in una politica esistente o in una dedicata, l'impegno a mantenere la conformità con i requisiti legali e contrattuali in materia di protezione dei dati personali. Vale la pena di segnalare che non tutti i controlli godono di questa estensione.

I capitoli 7 e 8, invece, riportano i principi enunciati all'interno della ISO/IEC 29100 come controlli aggiuntivi contestualizzati a un'applicazione da parte dei titolari (capitolo 7) e dei responsabili (capitolo 8) del trattamento di dati personali.

L'impiego dei contenuti dei capitoli 6, 7 e 8 è, come si evince dai loro titoli, **interamente opzionale**. Si tratta infatti di aggiunte ai controlli della ISO/IEC 27002 che possono quindi essere o non essere attuati sulla base dei risultati della valutazione e del successivo trattamento del rischio, che in questo caso è assolutamente importante che non sia solo relativo alla sicurezza delle informazioni ma anche alla tutela dei diritti e delle libertà degli interessati.

Vi sono infine ben 6 appendici che forniscono dei comodi schemi di riferimento per i capitoli 7 e 8 o vanno a mappare la ISO/IEC 29100, il GDPR, la ISO/IEC 27018, la ISO/IEC 29151 e a fornire linee guida su come utilizzare la norma stessa.

Vale la pena notare che la norma non può essere utilizzata indipendentemente ma è necessario fare uso congiunto di una copia della ISO/IEC 27001 e di una copia della ISO/IEC 27002, in quanto si è deciso in fase di produzione della stessa di non ripetere il testo di queste ultime ma di includere nel testo solo le modifiche differenziali alle stesse.

La ISO/IEC 27701, considerando anche i validissimi *editor* messi in campo tra cui lo stesso della fortunata BS 10012, è senza dubbio uno **strumento sofisticato**, ben integrato con il

parco normativo internazionale esistente e di potenziale interesse per tutte le organizzazioni dotate di un sistema di gestione per la sicurezza delle informazioni già solo per il fatto che molte di queste tratteranno inevitabilmente dei dati personali interni o di clienti. La sua stessa sofisticazione, d'altro canto, la rende un oggetto utilizzabile correttamente solo da una piccola porzione del mercato potenzialmente interessato da una certificazione secondo l'articolo 42 del GDPR, proprio per la **limitata diffusione dei sistemi di gestione per la sicurezza delle informazioni** (da fonti ISTAT e Accredia, circa 1 su 4500 in Italia), con particolare riferimento alle PMI. Un altro ostacolo in questo senso è costituito dallo schema di accreditamento utilizzato, coincidente con la ISO/IEC 17021 della ISO/IEC 27001 e diverso dalla più estesa ISO/IEC 17065 prescritta dall'articolo 43 del GDPR che, oltre ai sistemi di gestione e ai servizi forniti tramite gli stessi, include anche i prodotti. A questo proposito SC 27 ha appena varato un periodo di studio per valutare eventuali **azioni correttive** in materia ma queste ultime, quali che siano, difficilmente saranno messe in pista prima di un anno.

Superato questo passaggio, per quanto quasi certamente la ISO/IEC 27701 sarà sottoposta all'EDPB per valutazione rispetto ad uno schema di certificazione Europeo, rimarrà molto probabilmente spazio per altri schemi, quali ad esempio l'italiana - e liberamente scaricabile - UNI PdR 43.2:2018 (http://store.uni.com/catalogo/index.php/uni-pdr-43-2-2018.html), purché siano più semplici, autoconsistenti e direttamente applicabili, soprattutto nel vastissimo mercato delle PMI.

Articolo a cura di **Fabio Guasconi**