ARTICOLO DI PUNTOSICURO

Anno 21 - numero 4400 di Mercoledì 06 febbraio 2019

La conformità alla ISO 27001 garantisce la protezione dei dati?

Un'analisi dei requisiti di sicurezza della norma ISO 27001 sulla sicurezza dei sistemi informatici: la norma garantisce i requisiti imposti nel regolamento europeo di protezione dei dati personali GDPR 679/2016?

Si chiama IAPP, ed è una associazione di professionisti della protezione dei dati, la associazione che ha condotto un affascinante studio comparato fra i requisiti di sicurezza imposti dalla norma internazionale ISO 27001 e requisiti di sicurezza posti dal regolamento generale europeo. Anche se indubbiamente vi sono molti punti di contatto, vi sono alcune aree in cui le indicazioni della norma sono alquanto diverse dalle indicazioni del regolamento; ciò impone un accurato e combinato studio, da parte di professionisti della sicurezza informatica e professionisti della protezione dei dati, per essere certi che i vantaggi della norma internazionale siano sfruttati al meglio, senza lasciare delle aree scoperte, nei confronti delle imposizioni del regolamento europeo.

Non v'è alcun dubbio che vi siano alcuni obiettivi comuni, vale a dire la riduzione dei rischi per i dati degli interessati, sia dal punto di vista di protezione dei dati stessi, sia dal punto di vista di accesso controllato. D'altro canto, il regolamento offre agli interessati tutta una serie di diritti, che sono in pratica ignorati dalla norma internazionale. Ecco perché un'analisi comparata delle varie aree coinvolte dalla norma e dal regolamento permette di evidenziare sei aree principali:

- l'area afferente alla sicurezza,
- l'area afferente alla notificazione di violazione dei dati,
- l'area afferente alla gestione dei fornitori,
- l'area afferente alla registrazione e documentazione dei trattamenti effettuati,
- l'area afferente al rispetto delle indicazioni dell'articolo 25, vale a dire protezione dei dati fin dalla progettazione e protezione per impostazione predefinita, ed infine
- l'area afferente ai diritti degli interessati.

È bene ricordare che il regolamento europeo apprezza indubbiamente il fatto che i trattamenti siano effettuati in conformità a processi approvati e certificati, ma questo potrebbe essere solo un punto di partenza e non costituire una automatica garanzia di piena rispondenza alle indicazioni del regolamento.

Le certificazioni sono menzionate più volte nel regolamento generale ed in particolare nel considerando 77, e nell'articolo 42, che è specificamente dedicato all'illustrazione degli schemi di certificazione.

Anche l'articolo 58, che illustra i poteri del Garante, conferma come le autorità di supervisione nazionali abbiano il potere di rilasciare certificazioni o autorizzare enti specializzati a rilasciare certificazioni specifiche.

La presenza di un ente di accreditamento nazionale, Accredia, in Italia, fa sì che sia possibile anche, per l'autorità garante nazionale, delegare a tale ente nazionale il compito di accreditare gli istituti di certificazione.

Proviamo ad esaminare insieme alcune aree critiche, per vedere se e come vi può essere sovrapposizione o distacco fra le indicazioni dei due documenti menzionati.

Cominciamo a parlare delle procedure afferenti alla violazione dei dati

Non v'è dubbio che la norma internazionale indichi, senza incertezze, il fatto che qualunque incidente afferente alla sicurezza deve essere tempestivamente individuato e messo sotto controllo. Tuttavia, il regolamento dà delle indicazioni differenti, a seconda che il tipo di violazione che si è verificato possa o meno richiedere la notificazione agli interessati coinvolti. In particolare, l'articolo 33 richiede che i titolari informino immediatamente all'autorità nazionale Garante, quando la violazione possa portare a un rischio per i diritti e le libertà di un interessato, mentre l'articolo 34 richiede che anche gli interessati vengano tempestivamente informati, in alcuni casi particolari.

La norma internazionale non fa alcun riferimento a queste procedure ed ecco perché è indispensabile che il responsabile della sicurezza informatica lavori in stretto contatto con il responsabile della protezione dei dati per far sì che il piano di emergenza, che è stato già pianificato e addirittura attivato, comprenda anche questi passi specifici.

Colgo l'occasione per ricordare ai lettori che l'articolo 29 Working party ha prodotto un prezioso documento che offre numerose esemplificazioni, circa il fatto che una violazione dei dati debba o meno essere notificata agli interessati coinvolti. Ad esempio una perdita di una chiavetta USB, sulla quale sono archiviati dati personali protetti da algoritmo crittografico, non deve essere comunicata agli interessati, i cui dati sono sulla chiavetta.

Le garanzie che debbono essere pretese da un fornitore di servizi informatici

La continuità della catena di sicurezza, che protegge i dati personali che l'interessato ha fornito al titolare, non deve presentare alcuna smagliatura, soprattutto quando questi dati, per vari motivi, possono essere comunicati a soggetti terzi che su di essi operano. È classico il caso in cui i dati vengono riversati su un cloud, gestito da uno specifico responsabile del trattamento, così designato dal titolare. L'articolo 28 del regolamento esplicitamente richiede che le garanzie di protezione dei dati si estendano, con apposite pattuizioni contrattuali, anche ad un fornitore di servizi informatici. Anche in questo caso, l'appoggiarsi ad un fornitore di servizi informatici, che disponga, a sua volta, di un'appropriata certificazione di sicurezza, rappresenta un elemento garantistico per il titolare, che sceglie questo fornitore.

Contrassegni dei dati e log degli accessi

La clausola 8 della norma ISO 27001 richiede che il responsabile la sicurezza informatica sia in grado di contrassegnare con estrema chiarezza i dati che tratta, in modo da avere a disposizione un data base continuamente aggiornato, con una chiara identificazione dei dati stessi e degli utilizzi consentiti. Delle sotto clausole successive richiedono anche che il dato venga contrassegnato in termini di livello di riservatezza, mentre la clausola 9 stabilisce le regole per una politica di accesso ai dati stessi.

Il rispetto dell'articolo 25 del regolamento

Ad esempio, un chiaro contrassegno dei dati, con particolare riferimento ai dati temporali, può costituire un prezioso aiuto, quando giunge il momento in cui i dati devono essere cancellati. Se manca un contrassegno temporale, sempre presente ovunque i dati si trovino, è possibile che le operazioni di cancellazione non avvengano con la compiutezza che il regolamento tassativamente impone. Nello stesso contesto si pone la chiara identificazione dei dati, che permette di verificare se i dati acquisiti sono veramente i minimi necessari per le finalità di trattamento indicate, oppure, come purtroppo accade, vi è una grande differenza fra l'esigenza di utilizzare i dati e le modalità di cattura.

È ancora molto diffuso il concetto, che viene sintetizzato in queste parole: "acchiappa tutti i dati che puoi e poi vedremo quali servono e quali no!".

I diritti degli interessati

È questo un tema del tutto ignorato nella norma ISO 27001; per contro, come i lettori ben sanno, ampio spazio viene dedicato a questi diritti nel regolamento. Chi scrive fa parte dell'organo tecnico di verifica delle attività di un primario istituto di certificazione. Durante le attività di verifica, in particolare riferite alle certificazioni in conformità a ISO 27001, più volte ho avuto modo di vedere come i valutatori, inviati presso le aziende certificate, ancora non abbiano pienamente recepito questi aspetti. È ben vero che i valutatori devono verificare la conformità con la norma internazionale, ma è altrettanto evidente, almeno ad avviso di chi scrive, che la visita ispettiva possa essere un'ottima occasione per sensibilizzare l'azienda coinvolta sulle migliorie da introdurre, per fare sì che una certificazione in conformità a ISO 27001 possa essere anche pienamente soddisfacente nei confronti di quanto previsto ed imposto dal regolamento generale europeo.

Ad esempio, il regolamento europeo prevede il requisito della portabilità dei dati personali e questo tema non è in alcun modo preso in considerazione specifica nella norma sulla sicurezza dei sistemi informativi. Un altro tema che merita l'avvio di una specifica collaborazione con il responsabile della protezione dei dati riguarda la cancellazione selettiva dei consensi. Com'è noto, ogni interessato ha diritto di modificare il proprio piano granulare di consensi, nella maggior parte dei casi ritirando alcuni consensi precedentemente emessi. A questo punto occorre che il sistema informativo sia in grado di individuare sollecitamente questi consensi e provvedere all'aggiornamento del profilo dell'utente, vale a dire dell'interessato coinvolto.

Allegato il documento di confronto (pdf)

Adalberto Biasiotti