PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 20 - numero 4327 di Mercoledì 10 ottobre 2018

# Volete davvero proteggere i dati personali: ecco la preziosa guida NIST

***Una serie di raccomandazioni mirate a proteggere la riservatezza di dati personali dal National Institute of Standard and technology.***

Il regolamento generale sulla protezione dei dati, recepito alla fine di agosto 2018, ha destato in molti titolari e responsabili del trattamento una elevata sensibilità alla protezione dei dati. Per la verità questa sensibilità avrebbe dovuto esistere fin dal lontano 1996, ma dicono i saggi che sia meglio tardi che mai!

Poiché lo stesso problema, seppure con dimensioni diverse, esiste anche negli Stati Uniti, il prestigioso National Standard of information and technology ha pubblicato una guida, articolata secondo la lucida impostazione anglosassone, che permette di guidare titolari e responsabili trattamento nell'impostare una efficiente ed efficace politica di protezione dei dati personali.

Uno dei motivi per cui è stata sviluppata questa guida discende dal numero crescente di violazioni dei dati, che ha portato alla perdita di milioni di dati nell'arco degli ultimi anni. È noto che queste violazioni sono pericolose sia per gli interessati coinvolti, sia per le organizzazioni coinvolte. Gli interessati possono essere danneggiati dal furto di identità o da ricatti elettronici, mentre le aziende possono perdere la fiducia del pubblico, essere esposte a responsabilità legali od a costi di messa sotto controllo della perdita.

Un approccio corretto è quello grazie al quale si imposta un programma di analisi di rischio e di messa sotto controllo dei rischi individuati.

Sotto questo aspetto, la norma internazionale ISO 31000 rappresenta un elemento di riferimento che nessuno può ignorare.

Il documento è proprio impostato in maniera da offrire una guida nella identificazione del rischio, connesso alla riservatezza dei dati personali, e alla successiva messa sotto controllo.

Anche se il documento è essenzialmente dedicata alle agenzie federali degli Stati Uniti, esso può essere utile per chiunque debba garantire la riservatezza dei dati personali, che gli interessati gli hanno affidato.

Ecco in breve le principali raccomandazioni riportate nella guida.



## Le organizzazioni devono innanzitutto identificare tutti i dati personali che esse gestiscono.

È evidente che non sia possibile proteggere correttamente dei dati personali, se non sappiamo se ne siamo in possesso. Come regola generale, il concetto di dato personale e interpretato in modo estremamente allargato, perché nulla osta a proteggere un dato non personale come se lo fosse, mentre la mancata protezione di un dato personale può creare le conseguenze negative, che abbiamo illustrato. Per dato personale s'intende ogni informazione riferita ad uno specifico individuo, sia di tipo anagrafico, sia

di tipo sanitario, educativo, finanziario e legato al rapporto di impiego.

Occorre fare attenzione anche al fatto che è possibile che un'informazione non sia direttamente collegata ad un soggetto specifico, ma sia relativamente facile effettuare successivamente, con vari strumenti, questa connessione.

## Le organizzazioni devono minimizzare l'uso, raccolta e la conservazione dei dati personali, sulla base di ciò che è strettamente necessario per le finalità del trattamento.

Nessuno può dimenticare come questa raccomandazione sia in tutto simile a quella riportata nell'articolo 25 del regolamento generale, laddove si raccomanda di minimizzare la quantità di dati raccolti. Per rispettare questa indicazione, è indispensabile che le organizzazioni effettuino periodicamente dei controlli sulla quantità e qualità dei dati raccolti, per essere certi che il principio sia costantemente rispettato.

Una diretta conseguenza di questa raccomandazione è quella di eliminare i dati personali, quando essi non sono più necessari, perché le finalità per le quali sono stati raccolti sono esaurite.

Le organizzazioni devono classificare i dati personali in funzione della loro criticità.

Non tutti i dati personali sono da proteggere allo stesso modo. È indispensabile stabilire delle linee guida per validare delle procedure, che possono classificare il livello di riservatezza, e quindi di protezione, da applicare ai dati. Il livello di riservatezza viene per solito suddiviso in tre categorie, bassa, media, alta, in conseguenza del danno potenziale che potrebbe risultare da un trattamento non appropriato di questi dati, sia da parte dell'organizzazione, sia a causa di un accesso non autorizzato da parte di soggetti terzi.

Il documento offre una lista di fattori che l'organizzazione deve prendere in esame per determinare il livello di riservatezza del dato.

Come esempio di questi livelli di riservatezza si illustrano i seguenti:

- le identificabilità, vale a dire la facilità con cui un dato personale può essere ricondotta ad uno specifico individuo,
- la quantità di dati personali raccolti, laddove la violazione di 25 dati personali, rispetto a 25 milioni, ha indubbiamente un impatto ben differente. Il livello di riservatezza deve essere adattato sulla base della quantità dei dati che potrebbero essere coinvolti in una violazione,
- la sensibilità del dato, che fa riferimento alla natura del dato; ed è evidente che un dato sanitario merita una protezione più elevata, rispetto all'indirizzo dello stesso soggetto,
- il contesto di uso, laddove le organizzazioni devono valutare le ragioni per le quali i dati sono stati raccolti, archiviati, trattati o comunicati a terzi. Il livello di riservatezza da assegnare ad un dato è direttamente proporzionale, ad esempio, al numero di soggetti ai quali dato potrebbe essere comunicato. Si pensi ad esempio ad un elenco di agenti di polizia che agiscono sotto copertura: è evidente che una violazione di questi dati, anche se in numero limitato, potrebbe avere conseguenze drammatiche per i soggetti coinvolti,
- gli obblighi di proteggere la riservatezza, vale a dire il rispetto di obblighi che ogni organizzazione ha, nei confronti dell'interessato, di cui sono stati raccolti i dati,
- l'accesso e la ubicazione dei dati, laddove le organizzazioni devono classificare i livelli di accesso al dato e la ubicazione dei dati stessi. Quando i dati vengono consultati spesso e da parte di molte persone, vi possono essere più opportunità di compromettere la riservatezza dei dati coinvolti.

# Le organizzazioni devono adattare le protezioni dei dati al livello di riservatezza individuato

È evidente che non tutti i dati personali debbano essere protetti allo stesso modo. Questa è la ragione per cui i responsabili delle organizzazioni devono introdurre dei livelli di sicurezza idonee e allineati con il livello di riservatezza che si vuole raggiungere.

Le misure di sicurezza che possono essere adottate sono numerose, come ad esempio:

- la creazione di politiche e procedure, che siano specialmente mirate a proteggere la riservatezza dei dati personali,
- l'addestramento dei soggetti coinvolti, che rappresenta una delle più efficienti ed efficaci misure di sicurezza, che oltretutto ha un costo relativamente contenuto. Nessun soggetto dovrebbe poter accedere ai dati, senza prima aver ricevuto uno specifico addestramento;
- la anonimizzazione dei dati personali, il che significa che deve essere possibile modificare i dati, seppure in modo reversibile, in maniera che anche l'accesso illegittimo al dato non potrebbe consentire ad un soggetto terzo di ricostruire il soggetto fisico, cui i dati si riferiscono. Questa tecnica è particolarmente efficace quando i dati vengono utilizzati per esami e correlazioni, e non devono essere individualmente analizzati;
- l'utilizzo di politiche restrittive di accesso ai dati, che oggi sono realizzabili con relativa facilità, grazie agli efficienti ed efficaci sistemi di controllo dell'accesso ai dati su supporto informatico;
- l'attuazione di sistemi di controllo per gli apparati mobili, laddove le organizzazioni possono impedire o limitare in modo incisivo all'accesso ai dati personali da parte di dispositivi mobili, che per solito presentano un rischio più elevato, rispetto ad apparati fissi o semi fissi, situati all'interno delle strutture fisiche dell'organizzazione;
- la adozione di protocolli sicuri di trasmissione, laddove le organizzazioni devono essere in grado di garantire un adeguato livello di protezione delle informazioni, anche durante le fasi di trasmissione; uno degli strumenti più efficaci è evidentemente l'adozione di protocolli di criptografia, prima che il dato venga trasmesso;
- l'effettuazione di audit periodici, grazie ai quali si può tenere sotto controllo il livello di riservatezza dei dati e prendere tempestive misure correttive.

# Le organizzazioni devono sviluppare un piano per la gestione della violazione dei dati personali.

Anche il regolamento generale europeo prevede disposizioni similari, perché purtroppo nessuno può affermare di essere esente da questo rischio.

Nessuno può dubitare del fatto che l'adozione di un efficiente ed efficace piano di gestione della violazione dei dati può ridurre le conseguenze sull'azienda e sugli interessati coinvolti. Il piano deve anche includere gli elementi che possono permettere di decidere se gli interessati coinvolti devono essere informati o meno. Ricordo ai lettori che nel regolamento europeo questa decisione deve essere assunta dall'autorità di supervisione nazionale.

# Le organizzazioni devono incoraggiare un elevato livello di coordinamento fra i responsabili della protezione dei dati, i responsabili della security, i responsabili informatici e gli uffici legali, per fronteggiare i problemi legati alla protezione dei dati.

È evidente che la protezione della riservatezza dei dati personali richiede un'elevata conoscenza dei sistemi informativi, della sicurezza di questi sistemi, della protezione dei dati e dei requisiti legali connessi. Le decisioni che riguardano la applicabilità o meno di una specifica disposizione di legge o di regolamento devono essere prese dal comitato, di cui fanno parte tutti gli esperti precedentemente elencati.

Questo stesso comitato potrà tenere sotto controllo le politiche aziendali, adattandole all'evoluzione della situazione, in modo che venga garantita la interpretazione corretta dei requisiti imposti da leggi e regolamenti.

NIST (PDF, 3.4 mb)

**Adalberto Biasiotti**



**www.puntosicuro.it**