DPS: punto di arrivo o falsa partenza?

di Marco Piermarini (piermarini aT gmail.com)

7 Ottobre 2006

Il presente

E' improbabile che sull'argomento DPS le aziende, affidatesi a consulenti "improvvisati" dell'ultima ora (spesso a digiuno della normativa) o a software online di dubbia funzionalità, si sentano ormai al sicuro grazie a quei fogli di carta, pochi o tanti che siano, con il loro bel timbro datato fine marzo. Difficile che si sentano a posto, o che non credano di essere esposte a rischi di alcun genere.
Questa sensazione esce sicuramente rafforzata dalla mancanza di organici controlli sul territorio, ora che tutta l'attenzione dell'opinione pubblica e degli enti di controllo è stata spostata sulle intercettazioni o sulle novità della finanziaria.
Ma questa calma è soltanto l'apparente tranquillità prima della tempesta, e molti rischiano di trovarsi impreparati ed essere sommersi dalla marea.
Segnali che confermano questo trend sono le comunicazioni per fax in fondo alle quali si aggiungono diciture del tipo "se entro 5 giorni dalla presente comunicazione non ci arriverà una vostra risposta riterremo valido il consenso al trattamento dei vostri dati", in assoluta contraddizione con la richiesta di un consenso esplicito ed in barba al fatto che deve sempre esser liberamente prestato e non può mai essere né tacito o né per fatti concludenti!

I rischi per le aziende

Ma senza voler creare una sterile polemica, appare comunque chiaro il rischio per le aziende: faccio il mio compitino e sono apposto con la legge. Forse questo può essere vero in un primo momento, in quanto anche gli organi preposti al controllo, nello specifico la guardia di finanza organizzata in nuclei specializzati, sono ancora in fase di formazione e quindi hanno una conoscenza spesso superficiale che potrebbe portare ad un analisi altrettanto formale.
Probabile che i primi controlli siano mirati al riscontro di quei quattro cinque elementi necessari per essere a norma e stare tranquilli: DPS, informativa, lettere d'incarico, buste chiuse contenenti le psw ed i famigerati archivi chiusi a chiave.
Premesso che non tutti hanno messo in atto questi adempimenti, appare comunque rischioso e deleterio fermarsi al compitino in quanto rischia di diventare soltanto un boomerang che rassicura, ma in concreto non esenta dalla sanzione. Basta infatti una singola misura non attuata per trovarsi esposti alle sanzioni, ed un elemento che come sempre è stato trascurato nell'analisi di molti consulenti e manager aziendali è quello fondamentale: la progettazione.

Il futuro: Progettare la sicurezza

Si ritiene che perdere tempo in business plan o progettazioni strategiche non sia utile, bensì sia foriero di confusioni e dubbi che possono distrarre dalla vera attività dell'azienda, che è il perseguimento del suo core business. Ebbene, per fortuna, inizia a crearsi una maggiore cultura imprenditoriale, che vede sempre di più le aziende interrogarsi sui motivi del raggiungimento o meno dei propri risultati con necessità di mettersi seduti e verificarne le cause.
Nella privacy, così come nella sicurezza aziendale, non ci si può improvvisare, si deve pianificare la propria sicurezza e la gestione delle informazioni, assets fondamentale nella moderna gestione societaria.
Ecco emergere la criticità di chi ha agito di impulso e non ha riflettuto su quanto stava attuando: non basta mettersi in regola con la privacy, serve fare una concreta analisi delle proprietà criticità e determinare quali informazioni c'è interesse a gestire e tutelare, facendo delle scelte che devono poi essere attuate in maniera conforme e che portano a diverse e non sempre scontate soluzioni.
In questa logica diventa basilare avere le capacità per compiere questi passi, inizialmente guidati da consulenti esterni, ma anche formando personale interno competente e capace di pianificare e mantenere operative le decisioni prese per rendere efficienti ed efficaci le misure adottate. Questo punto di arrivo non è così semplice da raggiungere e serve una profonda

analisi per comprenderne la necessità e vederne i vantaggi.

Obblighi di legge: come soddisfarli

Non è un caso che il Codice della privacy D.lgs. 196/03, preveda l'obbligo formativo nell'allegato B, dedicato alle misure minime da adottare in azienda, dove si precisa:
"*19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.*"
Un simile approccio risulta difficile da individuare nel 90% delle aziende, per le quali la formazione risulta un di più inutile e poco produttivo che sottrae il personale dall'attività lavorativa vera e propria e costa dunque due volte all'azienda. Per questo è più facile che si segua il percorso storico già messo in atto con la legge 626/94 per la quale, dopo diversi interventi legislativi, si sono resi obbligatori e codificati con chiarezza gli interventi formativi specifici per ogni figura aziendale con il dettaglio della durata oraria minima, degli argomenti trattati per le varie funzioni e della cadenza del loro ripetersi.

Diversi interrogativi sulla formazione....

Nell'attesa di questa inevitabile conclusione rimane aperto il problema: con che criteri fare formazione sulla privacy?
La risposta potrebbe essere semplicistica e prevedere l'uso di comunicazioni interne con documenti scritti sull'argomento, magari scaricati da internet, e verbali controfirmati dai dipendenti per presa visione, pratiche forse sufficienti a soddisfare un primo e superficiale controllo da parte delle autorità. Ma in realtà questo tipo di approccio poteva essere sufficiente per il primo anno di vigore della normativa, per il secondo ormai alle porte, come posso attestare l'attenzione e la disponibilità dell'azienda ad implementare la sicurezza e a mantenere alta l'attenzione con relativa formazione degli incaricati?
Devo fare formazione, questa è l'unica risposta possibile, ma la più difficile anche da attuare. Dove e chi la eroga? Cosa mi serve? Come posso spendere in maniera adeguata i miei soldi e chi devo mandarci dei miei dipendenti? Quali sono i ruoli strategici della mia azienda?
Anche queste domande, se poste, possono trovare molteplici risposte, che avremo il piacere di trattare in un successivo articolo. Per ora vi segnalo soltanto un altro elemento che ritengo sia utile prendere in considerazione: perché limitarsi a soddisfare l'obbligo legislativo ed invece non trasformare una spesa inevitabile in un vantaggio strategico sia per al gestione interna che a livello di immagine. Di cosa sto parlando?

....un unica risposta: ISO 27000

Della possibilità di andare oltre e definire una strategia societaria che vede l'adempimento trasformarsi in un occasione di crescita, investendo per iniziare l'adeguamento agli standard della ISO 27001 e successivi, con il vantaggio che svolgere formazione in quell'ambito porta un vero vantaggio strategico nella inevitabile consapevolezza che un domani sarà lo standard per tutti. Se volete saperne di più, date uno sguardo qui.
Si deve considerare questo aspetto: per poter capire come gestire la sicurezza devo prima sapere di cosa si parla altrimenti mi è impossibile scegliere in modo consapevole e avere un investimento efficace, sia esso in formazione che nell'acquisto di altri strumenti.

Marco Piermarini