Domande e risposte

Chi controlla che le misure minime e gli altri adempimenti previsti dalla legge sono messi in pratica?
La Polizia Postale (con le sue 76 Sezioni sul territorio) e la Guardia di Finanza in forza di un protocollo di intesa con il Garante.

Se esiste una autorizzazione generale al trattamento dei dati, è possibile trattare i dati senza il consenso dell'interessato?
No, è solo possibile omettere la notifica al Garante e si può procedere con il trattamento dei dati, osservando tutte le prescrizioni.

E' vero che è obbligatorio per tutte le organizzazioni avere un DPS (Documento Programmatico della Sicurezza)?
No! Il D.P.S. è obbligatorio (Art. 34 del Testo Unico) solo per quelle organizzazioni che trattano dati personali (anche non sensibili) con l'impiego di elaboratori elettronici. Chi tratta i dati solo manualmente su supporto cartaceo, non è tenuto ad avere il DPS.

E' obbligatorio preparare un D.P.S. (Documento Programmatico sulla Sicurezza) che contenga una analisi dei rischi?
Si, è esplicitamente richiesto dal comma 19.6 dell'Allegato B del D.Lgs. 196/03 per tutte le organizzazioni che trattano dati sensibili con l'ausilio di elaboratori elettronici.

A cosa serve il Documento Programmatico della Sicurezza (DPS)?
Il Documento Programmatico per la Sicurezza identifica gli aspetti dell'infrastruttura tecnologica aziendale coinvolti nella gestione di dati personali e sensibili, verificandone l'aderenza a quanto disposto dalle più recenti normative (Dlgs. N.196 del 30 Giugno 2003). Inoltre, il DPS definisce e descrive le misure necessarie per una vera "messa in sicurezza" del sistema informativo aziendale.

Il documento è solo un adempimento legale?
Il documento rappresenta non solo un adempimento legale ma un vero e proprio strumento di riferimento per l'azienda in materia di trattamento dei dati personali, e in generale di definizione delle strategie di sicurezza, e delle conseguenti policy che tutti i dipendenti, collaboratori, partner e fornitori devono adottare.

Quali sono i risultati per il Cliente di un progetto DPS ?
Il DPS evidenzia i punti di forza e di debolezza dell'infrastruttura esistente, evidenziando anche i rischi normativi (legati ad eventuali inadempimenti richiesti dalla legge) e funzionali (legati al proprio modello di business derivanti da una gestione della sicurezza non ottimale). Formalizza inoltre le policy di lavoro, costituendo un valido riferimento per l'utilizzo dell'infrastruttura informativa, e formalizza le procedure di intervento in caso di problemi o guasti.

Non siamo collegati ad internet, non siamo già sicuri?
No. Il collegamento ad internet è solo una delle minacce e neanche la più importante. Secondo le statistiche di istituti di ricerca e polizie, circa tre quarti degli incidenti sono generati all'interno delle organizzazioni. Di questi, oltre la metà sono involontari, perchè... "errare è umano".

Possiamo scegliere di ignorare questo dispositivo di legge e correre il rischio?
No. La sensibilità dell'opinione pubblica sul tema della privacy è molto alta. Se le probabilità di ricevere un'ispezione da parte degli ispettori del Garante della Privacy sono basse, in caso di incidenti anche banali (p.e. il furto di un disco o di un computer contenente dati personali nella vostra azienda) potreste non essere in grado di dimostrare che trattavate i dati in conformità alla legge. In questo caso vi esponete al rischio di sanzioni anche penali (e la responsabilità penale è personale).

Le misure minime di sicurezza richieste dal Dlgs.196/2003 non sono esagerate rispetto alle necessità ed alle possibilità di una piccola azienda?
No. Probabilmente molte delle misure richieste dalla legge sono già prassi comune nella vostra azienda. Ai fini della conformità al Codice della Privacy , si tratta per lo più di formalizzare quanto già fate grazie al Documento Programmatico sulla Sicurezza. Eventuali misure addizionali non sono di norma molto onerose ne da un punto di vista economico ne da un punto di vista organizzativo.

I dati personali che abbiamo li facciamo elaborare da uno studio esterno, non è lui il titolare?
No. Anche se tutti i trattamenti (per esempio di paghe e contributi o contabili) sono effettuati all'esterno, i titolari di quei trattamenti siete voi e quindi voi ne risponderete in merito alla loro privacy e sicurezza.

La nostra rete è protetta dal "firewall", non siamo già sicuri?
No. Il firewall è un dispositivo utile, ma che, quando ben gestito, svolge solo una funzione ben precisa: proteggere la vostra rete informatica aziendale da specifici tipi di incidenti di origine esterna. Questo ha poco a che vedere con la Privacy ed il Dlgs.196/2003, che in particolare mira anche a proteggere i dati personali (informatici e non) e la vostra azienda sia da incidenti interni che esterni, deliberati o accidentali. Per esempio, il firewall non vi serve a proteggere i dati in caso di perdita accidentale per guasto o furto del computer e tantomeno a proteggere i vostri archivi cartacei dalle conseguenze di un incendio.