Domande & Risposte

Cos'è il D.P.S. Documento programmatico sulla Sicurezza?
Il D.P.S. è l'unico documento in grado di attestare l'adeguamento alla normativa sulla tutela dei dati personali (privacy) e deve essere redatto entro il 31 MARZO 2006 ed alla scadenza fissata al 31 di marzo di ogni anno. Il DPS è un manuale per la pianificazione della sicurezza dei dati in azienda / studio professionale / organizzazione: descrive come si tutelano i dati personali di dipendenti, collaboratori, clienti, utenti, fornitori ecc. Il Garante ha individuato una figura responsabile per il trattamento dei dati più una serie di punti per i quali l'azienda deve adottare tutte le misure necessarie per l'espletamento della legge. Lo scopo del D.P.S. è proprio quello di descrivere la situazione attuale con riferimento ai punti stabiliti dal garante.
I tempi di stesura del DPS variano a secondo della dimensione dell'azienda e dalla mole di dati da processare, certamente non ci si mette un giorno... il documento programmatico richiede una attenta valutazione della situazione aziendale e dei trattamenti effettuati.

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 programmatico sulla sicurezza è realmente necessario?
Il Documento Programmatico sulla Sicurezza è obbligatorio per tutti coloro che trattano dati sensibili con l'impiego di elaboratori elettronici. Tuttavia sia per il fatto che spesso esso vengono trattati inconsapevolmente sia perché larga parte del lavoro riepilogato nel DPS va comunque affrontato anche per i soli dati comuni trattati in forma elettronica, è consigliato per tutte le Aziende.

Il DPS 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.

Perché è consigliato in ogni caso, per tutte le aziende?
E' consigliato sempre in quanto si tratta di un "piano di sicurezza" che può essere comunque utile, soprattutto in vista di possibili azioni civili, come elemento di prova dell'adozione di "tutte le misure idonee".

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.

Domande & Risposte

Chi deve adeguarsi alla legge sulla Privacy?
Qualsiasi persona giuridica pubblica o privata (azienda, professionista, associazione, ente, ecc.) che tratti dati personali di terzi (clienti, dipendenti o fornitori ecc.) nell'esercizio della propria attività professionale è obbligata ad adottare tutte le misure minime di sicurezza richieste dal nuovo Codice affinché venga tutelata la riservatezza e la sicurezza dei dati personali contenuti negli archivi. Questi dati sono intesi sia archiviati elettronicamente che in qualunque altro modo, incluso il cartaceo. In pratica, sono escluse dall'adeguamento al Nuovo Codice **solo le persone fisiche** che effettuano il trattamento di dati personali per **soli fini personali** e, in nessun caso, prevedano la cessione o la comunicazione a terzi dei dati in loro possesso

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 sia da un punto di vista economico sia da un punto di vista organizzativo.

Non siamo collegati ad internet, non siamo già sicuri?
No. Il collegamento ad internet è solo una delle minacce e neppure 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.

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.

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.

Domande & Risposte

Qual è la differenza tra dati comuni, sensibili e giudiziari?
Dati comuni: nome, cognome, telefono, fax, codice fiscale, partita Iva, etc.
Dati sensibili: dati idonei a rilevare origine razziale, convinzioni religiose, opinioni politiche, stato di salute, vita sessuale, etc.
Dati giudiziari: dati relativi al casellario giudiziale, qualità di imputato o indagato, oppure atti di causa / perizie in sede civile, penale, stragiudiziale.

Chi sono gli incaricati?
Tutte le persone fisiche che hanno accesso ai dati a vario titolo devono essere designate per iscritto quali incaricati del trattamento.

Cosa sono le "Lettere di Incarico"?
Le Lettere di Incarico sono documenti formali ed obbligatori che la normativa privacy impone per la nomina dei Responsabili e degli Incaricati interni (dipendenti) ed esterni al trattamento dei dati.

E' vero che la documentazione cartacea deve essere protetta in "armadi ignifughi"?
Non necessariamente. Il cartaceo può essere archiviato in normali armadi e/o cassetti il cui accesso (la chiave) è posto sotto la il controllo del Responsabile della Sicurezza.
E' altresì vero che devono essere rispettate le opportune misure antincendio, già previste peraltro dalla normativa sulla sicurezza sul lavoro (D.Lgs 626/94)

Chi controlla gli adempimenti previsti dalla legge siano messi in pratica? I controlli vengono effettuati dalla Polizia Postale e dalla Guardia di Finanza sulla base di un protocollo di intesa con il Garante.

Il DPS deve essere riscritto tutti gli anni?
Il DPS non deve essere totalmente riscritto tutti gli anni ma deve invece essere aggiornato entro il 31-03 di ogni anno.