Il DPS: cos'è e come si aggiorna.

Di Marco Maglio
Mercoledì 14 Marzo 2007 18:16

Il 31 marzo scade il termine per l'aggiornamento annuale del Documento Programmatico sulla sicurezza. Già da un anno, con la definitiva entrata in vigore del nuovo codice per il trattamento dei dati personali, un ruolo centrale nella gestione della sicurezza informatica è svolto dal Documento Programmatico per la Sicurezza (DPS) che è indicato come una delle misure minime di sicurezza per il corretto trattamento dei dati. Con le nuova norme, molto più stringenti di quelle previste dalla vecchia normativa risalente al 1999, il DPS è diventato un obbligo per tutte le organizzazioni, pubbliche e private, che trattano dati sensibili con l'uso di strumenti elettronici: è sufficiente che dei dati risiedano su un singolo PC, anche se questo non è collegato ad alcuna rete, perché il DPS diventi obbligatorio. Il DPS ha anche una importante funzione interna di guida all'adozione ed al miglioramento delle misure di sicurezza perché permette di verificare livello di sicurezza informatica aziendale e di identificare subito le aree maggiormente a rischio. La specificità delle strutture nei diversi soggetti fanno sì che il DPS non sia un documento uguale per tutti, ma il frutto di una valutazione specifica da parte delle singole aziende. Per questo motivo, il Codice sulla Privacy sancisce l'obbligatorietà di interventi formativi per gli incaricati del trattamento dei dati personali. La formazione dovrebbe essere programmata già al momento dell'ingresso in servizio ed in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti per il trattamento di dati personali. Le aziende per predisporre misure minime di sicurezza devono definire preventivamente i limiti di utilizzo degli strumenti informatici da parte dei dipendenti. Da questo punto di vista gli imprenditori dovrebbero porsi queste domande fondamentali: • è possibile controllare il corretto uso da parte dei propri dipendenti del personal computer e dei relativi programmi? • quali regole e quali tecnologie possono essere studiate per garantire al lavoratore il rispetto della sua riservatezza ed all'azienda il diritto di esercitare il suo potere di controllo nell'ambito della gestione del rapporto di lavoro? Non si tratta di questioni di poco conto anche perché le risposte da fornire devono bilanciarsi con i limiti imposti dalla normativa in materia di diritti alla riservatezza e di divieto dei controlli a distanza sull'attività dei dipendenti. Il rischio che tali controlli possano essere considerati illegittimi ai sensi dello statuto dei lavoratori è alto. Proprio in questo momento, in cui la legislazione non riesce a tenere il passo con lo sviluppo della tecnologia, l'azienda dovrà adottare una politica aziendale trasparente, anche attraverso

l'elaborazione di regolamento aziendale che limiti l'uso improprio degli strumenti informatici da parte dei dipendenti. Per un ripasso rapido su questa materia, senza perdersi in tecnicismi ecco un percorso in sei domande e risposte per verificare rapidamente come gestire questa essenziale misura di sicurezza per il trattamento dei dati personali 1) Che cos'è il Documento programmatico sulla sicurezza Il documento programmatico è una delle misure minime di sicurezza prescritte dalla normativa per gestire correttamente i rischi connessi al trattamento dei dati personali. Le misure di sicurezza hanno lo scopo di prevenire i rischi di distruzione, intrusione o uso improprio dei dati personali. Alle precauzioni già previste nella normativa fin dal 1999 (password, codici identificativi, utilizzo di antivirus aggiornati) con l'adozione del Codice in materia di protezione dei dati personali, dopo il 31 marzo 2006, sono state aggiunte anche forme di autenticazione informatica, sistemi di cifratura, procedure per il ripristino dei dati da adottare a seconda della sensibilità e del livello di rischio legato al trattamento dei dati. Nel caso in cui il titolare ometta l'adozione delle misure minime è prevista la pena dell'arresto sino a due anni o, alternativamente, l'ammenda da euro 10.000 a 50.000. 2) Il DPS è obbligatorio per chiunque? Secondo l'allegato B del D.lgs 196/2003 il documento è obbligatorio solo per i soggetti che trattano dati sensibili e giudiziari ma la sua adozione è essenziale per l'adeguata analisi e prevenzione dei rischi legati all'illecito trattamento dei dati. Non redigere il DPS determina l'automatico innalzamento dei rischi connessi la trattamento. Per questo motivo la sua redazione, anche se non rigorosamente obbligatoria è da considerarsi una necessaria cautela da adottare per la corretta organizzazione. In un quadro di evoluzione tecnologica costante, il DPS va aggiornato almeno una volta all'anno, entro il 31 marzo, da parte del Titolare, anche avvalendosi dei responsabili eventualmente designati. Dell'avvenuta redazione va data notizia nella relazione accompagnatoria al Bilancio. Ai sensi della regola 26 dell'Allegato B del D.il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza. 3) Il Documento programmatico deve avere data certa? Non esiste nessuna disposizione che preveda un obbligo di data cera per il DPS. La diffusione di una "leggenda metropolitana" a questo proposito deriva da una frettolosa lettura della normativa. L'unico riferimento alla data certa riguarda l'ipotesi (oggi superata) di usufruire di un maggior termine per l'adozione delle misure di sicurezza. Ai sensi dell'Art. 180 del D.lgs 196/2003 " Il titolare che alla data di entrata in vigore del presente codice dispone di strumenti elettronici che, per obiettive ragioni tecniche, non consentono in tutto o in parte l'immediata applicazione delle misure minime di cui all'articolo 34 e delle corrispondenti modalità tecniche di cui all'allegato B), descrive le medesime ragioni in un documento a data certa da conservare presso la propria struttura." 4) Qual è il contenuto del DPS? il DPS deve fornire idonee informazioni riguardo a : a) l'elenco dei trattamenti di dati personali; b) la distribuzione dei compiti e delle responsabilità in relazione al trattamento dei dati; c) l'analisi dei rischi; d) le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché le disposizioni per la protezione dei locali destinati alla custodia; e) la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento; f) la previsione di interventi formativi a favore degli incaricati del trattamento; g) la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare; h) l'individuazione dei criteri da adottare per la cifratura o per la separazione dei dati relativi alla salute ed alla vita sessuale dagli altri dati personali dell'interessato. Questo punto riguarda peraltro quasi esclusivamente gli organismi sanitari e gli esercenti professioni sanitari 5) Quando bisogna aggiornare il DPS? La revisione

del documento deve essere fatta entro il 31 marzo di ogni anno. Se nulla è cambiato rispetto alla situazione precedente, in via precauzionale, è opportuno quanto meno ristampare lo stesso documento con il nuovo numero di revisione e la data (possibilmente, anche se non è obbligatorio, dandogli data certa). Al di là dell'obbligo di legge di procedere ad un aggiornamento del documento entro il 31 marzo di ogni anno, è opportuno stampare una nuova revisione del documento ogni volta che qualche elemento contenuto nel DPS varia (anche più volte l'anno, se opportuno), ossia, quando vi siano innovazioni tecnologiche o modificazioni di processi organizzativi aziendali. Inoltre è bene tenere presente che il DPS, per sua specifica natura, ha carattere ricognitivo, nel senso che deve descrivere la situazione attuale rispetto alle misure di sicurezza. Inoltre il documento deve essere mirare a programmare interventi futuri per la protezione dei dati e dei sistemi informatici e fisici adottati per la protezione delle informazioni. Proprio per questo si deve verificare se nel corso dell'anno sono stati evidenziati rischi o minacce (ripetendo l'analisi dei rischi), in modo da prevedere interventi e protezioni. Va poi tenuto presente che oltre all'obbligo di aggiornamento annuale gli amministratori sono tenuti altresì a riferire dell'avvenuto aggiornamento nella relazione accompagnatoria al bilancio di esercizio. Questo spiega anche il legame con il bilancio e la previsione di un termine che è perfettamente aderente con la programmazione aziendale della gestione delle risorse e dei budget. Proprio per questo motivo la scelta operativa migliore consiste nel programmare per tempo gli interventi: a settembre si può iniziare a lavorare al documento preventivo e a marzo, sulla base delle previsioni, si può aggiornare il DPS. In questo modo l'aggiornamento annuale obbligatorio si effettua un semestre dopo le previsioni dell'anno precedente, e un semestre prima di quelle per l'anno successivo ed in prossimità del bilancio consuntivo. 6) Quali formalità occorre rispettare effettuando l'aggiornamento annuale? Il legislatore non dà nessuna indicazione circa la forma nella quale esso deve avvenire. Quello che è certo è che, almeno una volta all'anno (entro il 31 marzo) occorre provvedere alla revisione del sistema di sicurezza, facendo menzione dell'avvenuta revisione nella relazione accompagnatoria al bilancio di esercizio (potrebbe anche non darsi corso ad alcun aggiornamento del sistema, perciò si dichiarerà che sono state adottate le misure minime previste dall'allegato B al Codice e che si è valutato di non dover adottare altre misure diverse da quelle già in essere). Va tenuto presente che se si riterrà necessario aggiornare il DPS, non sarà necessario adottarne uno completamente diverso rispetto al precedente, ma basterà integrarlo in alcune parti, secondo le proprie necessità, ovvero si potrà sostituirlo integralmente con un documento diverso. Sul piano pratico un buon suggerimento può essere quello di adottare un modello di DPS (simile a quelli dei sistemi qualità secondo le norme ISO), composto di una parte descrittiva (da lasciare generalmente immutata) e da una serie di allegati, costituenti la parte dinamica, che riporterà le modifiche, le revisioni, gli aggiornamenti e le integrazioni ritenute necessarie.