

DPS obbligatorio per tutti i trattamenti elettronici di dati!

di Andrea Lisi (www.scint.it - www.studiodl.it) e Valentina Frediani (www.consulentelegaleinformatico.it) -

Il Documento Programmatico sulla Sicurezza obbligatorio per tutti coloro che trattano elettronicamente dati personali. Ecco perché

11/06/04 - Roma - Scade il 30 giugno il termine per la redazione del documento programmatico sulla sicurezza dei dati (di seguito anche D.P.S. (1)). Ma l'interrogativo che si/ci pongono varie società e professionisti è se la redazione sia obbligatoria solo per chi fa trattamento elettronico di dati sensibili e/o giudiziari o anche per chi fa, in generale, il trattamento elettronico di dati personali.

Per rispondere occorre visionare nella sua globalità sia il codice in materia di protezione dei dati personali (D.Lgs. 196/03), sia l'allegato B) al codice, recante il disciplinare tecnico in materia di misure minime di sicurezza. Infatti, dalla lettura del codice emerge chiaramente che alcune misure di sicurezza "minime" (tra le quali rientra la redazione del D.P.S.) debbono essere adottate per i dati personali trattati in formato elettronico, e per i dati sensibili, sia trattati in formato elettronico sia in formato cartaceo.

In particolare, sembra eliminare qualsiasi tipo di dubbio l'art. 34 del codice, il quale al punto g) dice espressamente e univocamente: "... il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime: ...g) tenuta di un aggiornato documento programmatico sulla sicurezza...".

L'articolo, quindi, non fa assolutamente riferimento in modo esclusivo ai dati sensibili o giudiziari, ma al contrario cita le misure di sicurezza minime riferibili ai dati personali in generale (e diversamente si è comportato il legislatore nel punto h) dello stesso articolo dove ha specificato che solo per alcuni dati inerenti la salute trattati da organismi sanitari occorre procedere al trattamento utilizzando tecniche di cifratura).

Taluni sono stati indotti in errore nella lettura interpretativa di tali norme dal disciplinare tecnico allegato al codice, il quale alla voce documento programmatico sulla sicurezza, ha espressamente stabilito: "Entro il 31 marzo di ogni anno, il titolare del trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile se designato, un documento programmatico sulla sicurezza contenente idonee informazioni...".

Ma basta leggere con attenzione la norma per sostenere che l'allegato tecnico, eventualmente, prevede soltanto che il DPS vada redatto per il trattamento elettronico di dati sensibili e/o giudiziari entro una certa data e, cioè, il 31 marzo di ogni anno, ma di certo tale asserzione non esclude l'obbligo generale di redazione del DPS in caso di trattamento elettronico di dati comuni (come indicato, si ripete, nell'art. 34 lett. g)! Altrimenti l'allegato tecnico comporterebbe una sorta di abrogazione implicita di un principio generale fornito nell'art. 34 e ciò costituirebbe veramente un curioso precedente nella tecnica normativa usualmente utilizzata dal nostro legislatore.

L'art. 34 – si ripete – prevede che “il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi – e non nei limiti! - previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime”, tra le quali il DPS.

Inoltre, dalla stessa voce del disciplinare tecnico emerge chiaramente al punto 19.1, ovvero in relazione all'obbligo di inserire nel documento programmatico determinati elementi, quello di inserire l'elenco dei trattamenti di dati personali: ed ecco perdersi nuovamente la distinzione tra dato sensibile o meno!

Infine, a favore della ovvia lettura della norma che preveda un obbligo generale di redazione del documento programmatico in capo a tutte quelle società, enti pubblici o studi professionali che gestiscano sia anagrafiche relative a clienti e fornitori, sia dati dei dipendenti, vi è la stessa ratio sottesa dal Codice per gli adempimenti inerenti alle misure di sicurezza: far evolvere la sicurezza nelle strutture aziendali o professionali attraverso l'imposizione di misure che siano concretamente capaci di ridurre la vulnerabilità della perdita o del danneggiamento di tutti i dati (comuni o sensibili che siano). Tanto che è logico prospettare che ogni società abbia il preciso obbligo di verificare la sussistenza delle misure minime di sicurezza all'interno della propria realtà, divenendo così il documento programmatico semplicemente una fotografia della sicurezza vigente nell'azienda con uno sguardo proiettato verso le misure che in un futuro prossimo appariranno adeguate non solo a livello normativo, ma soprattutto alla luce della necessità della struttura aziendale stessa di preservare il proprio patrimonio fatto sostanzialmente di dati (e, infatti, si parla di documento programmatico sulla sicurezza).

Per concludere, poniamo a tutti una domanda provocatoria: chi può con tranquillità sostenere di essere totalmente sicuro di trattare nel proprio sistema informatico solo e soltanto dati comuni e non anche sensibili (2)? E nell'incertezza è giusto forse rischiare le pesanti sanzioni previste dal legislatore in caso di violazione dell'obbligo di adozione di misure minime di sicurezza (arresto sino a due anni o ammenda da diecimila euro a cinquantamila euro ex art. 169 del Codice)?

avv. Valentina Frediani
Consulentelegaleinformatico.it

avv. Andrea Lisi
Studio Legale Lisi

NOTE

(1) Per un approfondimento della materia si consiglia la lettura dell'articolo "I nuovi faticosi adempimenti del Codice della Privacy per Pubbliche Amministrazioni, Imprese e Professionisti. Il Documento Programmatico sulla Sicurezza serve un po' a tutti coloro che trattano elettronicamente dati personali...e non solo a loro!", a cura di A. Lisi, visibile alla pagina http://www.scint.it/appr_new.php?id=109

(2) La definizione di dati sensibili fornita dalla legge è così vasta che possono rientrarvi molti dati personali che trattiamo quotidianamente (anche, in alcuni casi, le stesse e-mail, qualora contengano direttamente o indirettamente dei "requisiti di appartenenza" a particolari categorie: es. e.mail tiziosempronio@partitopolitico.it)